SEGURIDAD EN SERVIDORES LINUX NOTA 2





REVISTA DE NETWORKING Y PROGRAMACIÓN

#23



Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.



Intelligent Security

SECCIÓN ESPECIAL

ALSI Academia Latinoamericana de Seguridad Informática

TECNOLOGIAS MOVILES

¿Por qué 3G?

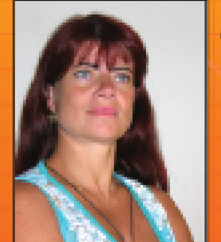
CRIPTOGRAFIA
Prueba de Conocimiento-Cero

EXAMEN
y Certificación
CISSP

HARDWARE
Servers en PYMES y Corporaciones

Seguridad en SQL 2005

INNOVADORES IT



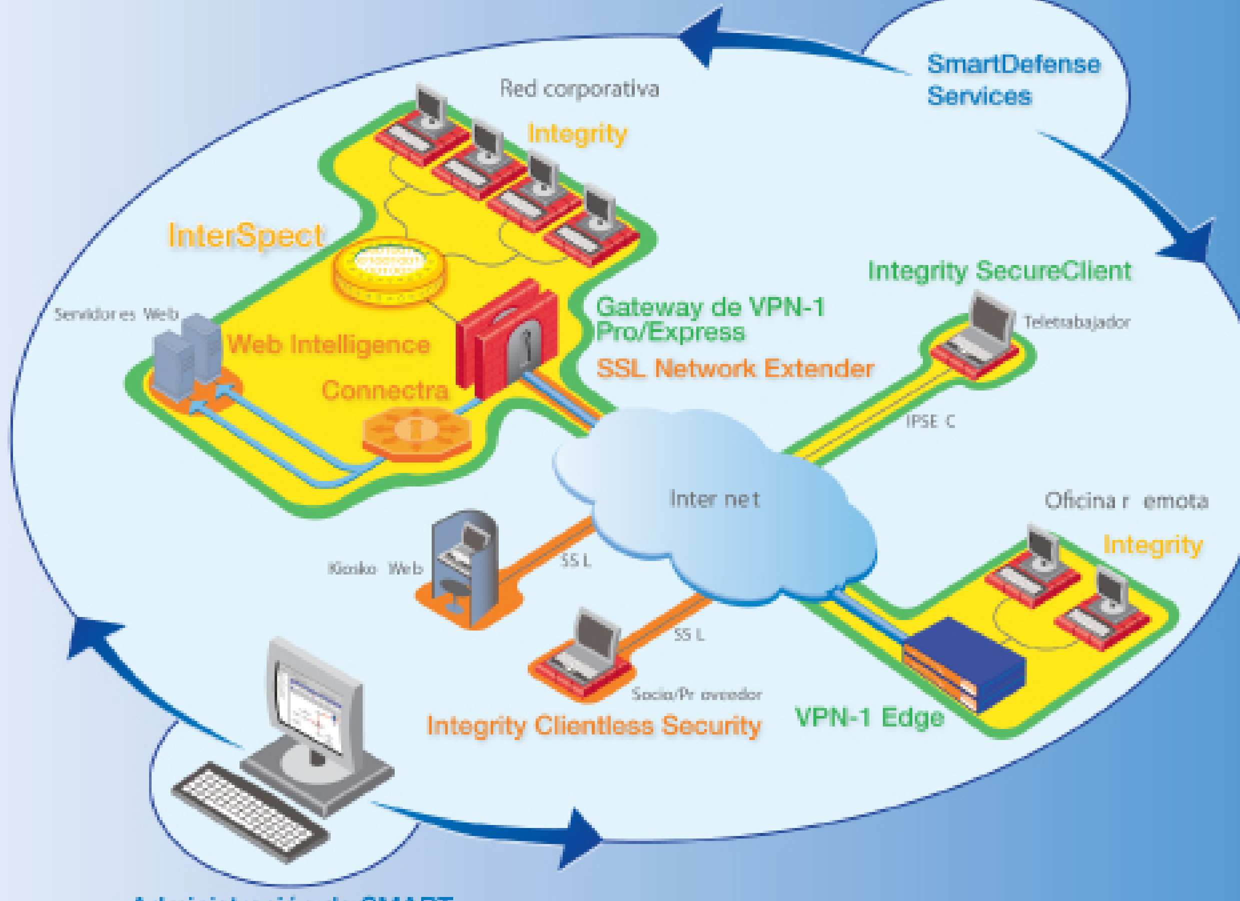
APRENDA CON LOS MEJORES
"Securizar es la base"
Conozcamos a Silvia Fandiño, IT Manager, Organon Argentina.

WWW.NEXWEB.COM.AR
ISSN 1668-5423
9 771668 542003 00023
Dist. Cap.: Vaccaro Sanchez y Cía. S.C. - Interior: DGP
Correo Argentino FRANQUEO A PAGAR Cta. 10188



Check Point

ofrece las soluciones de seguridad más inteligentes del mundo.



Administración de SMART
Administrador de eventos de seguridad de Eventia

Check Point es la única empresa que conoce a la perfección los problemas de la seguridad. Sólo Check Point dispone de las soluciones.

Póngase en contacto con nosotros
Oficina Mundial
Check Point Software Technologies Ltd.
3A Jabotinsky St., Diamond Tower
Ramat Gan, 52520 Israel
Tel.: +972-3-753-4555
Fax.: +972-3-575-9256
Correo electrónico: info@checkpoint.com

www.checkpoint.com





DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

COORDINADOR EDITORIAL
- Carlos Rodríguez Bontempi

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

DIRECTOR COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

EDITORES
- Carlos Vaughn O'Connor
- Carlos Rodríguez

EDITOR TÉCNICO
- Alejandro Cynowicz
redaccion@nexweb.com.ar

DISTRIBUCIÓN
- Mariano H. Agüero
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
- Andrés Vázquez
- Martín Guaglianone
suscripciones@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- DCV Esteban Báez
- Carlos Rodríguez Bontempi

PREIMPRESIÓN E IMPRESIÓN
IPESA Magallanes 1315. Cap. Fed.
Tel 4303-2305/10

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Vaccaro, Sánchez y Cia. S. C. Moreno 794, Piso 9. C1091AAP- Capital Federal Argentina.
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1 C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Si desea escribir para nosotros, enviar un e-mail a:
articulos@nexweb.com.ar



Nota del Editor

A partir de NEX #21 Check Point Software Technologies (www.checkpoint.com) tuvo una pauta de publicidad en nuestra revista. Cuando comenzamos a planear NEX #23 nos surgió la idea de solicitarles poder contar con un artículo redactado por algún experto de Check Point.
Cuando contactamos a Carina Strobietto, Check Point Product Manager - Cono Sur - Licencias Online: Distribuidor Mayorista de Software por ésto, nos sugirió de porqué no tener varios y hacer un "especial" con una serie de artículos.
Estamos orgullosos, de haber podido concretar esta acción y ofrecerles a nuestros lectores, en este número de NEX un "Especial Check Point". Éste consta de varios artículos que por un lado nos cuentan la historia y misión de la empresa, líder mundial en software de seguridad en Internet incluyendo VPNs y Firewalls de seguridad. El lema que conduce a Check Point es "We Secure the Internet" y en ese segmento los productos y tecnologías que los conforman no pueden ser superados.
Nuestros lectores deben conocer la empresa. Pero, también saber ¿Cómo nació?, ¿Quién es Gil Shwed?, ¿Cuáles han sido sus contribuciones al mundo de la seguridad informática?
Recomendamos leer el especial Check Point para aprender de productos, tecnologías y gente.

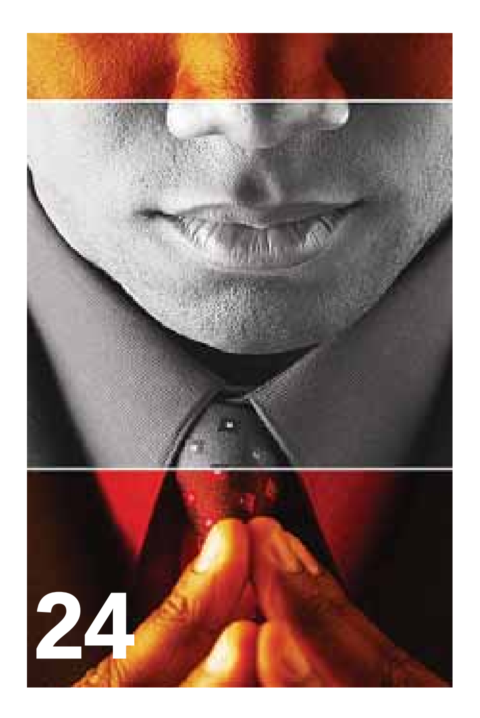
¿Qué novedades más componen NEX #23?

1. Mucho se habla de la convergencia de redes móviles y fijas. En NEX #22 dimos detalles de las tecnologías detrás de Wireless e IP. Nuestro tema de tapa en NEX #23, "Tecnologías Móviles", nos cuenta una radiografía de su presente y futuro.
2. Inauguramos la serie de artículos sobre "Tendencias en Desarrollo de Software" en colaboración con Snoop Consulting.
3. En innovadores en IT conocemos a Silvia Fandiño, IT Manager, Organon Argentina.
4. Seguridad en Servidores Linux presenta su Nota #2 de 5.
5. Inauguramos una serie sobre Hardware.
6. Muchos de Uds. habrán escuchado de la certificación CISSP de seguridad informática. Conceptos como que "es la más prestigiosa", "abarca numerosos temas pero no con mucha profundidad", "se basa en 10 CBK (Common Base Knowledge)", etc. Pero, ¿Cómo es un examen CISSP?.

Y como siempre hay artículos de mucho interés y vigencia para el IT pro, el experto de seguridad, los desarrolladores y networkers.

Vuestro feedback nos orienta y estimula, no dejen de enviar sus comentarios a *redaccion@nexweb.com.ar*

SUMARIO



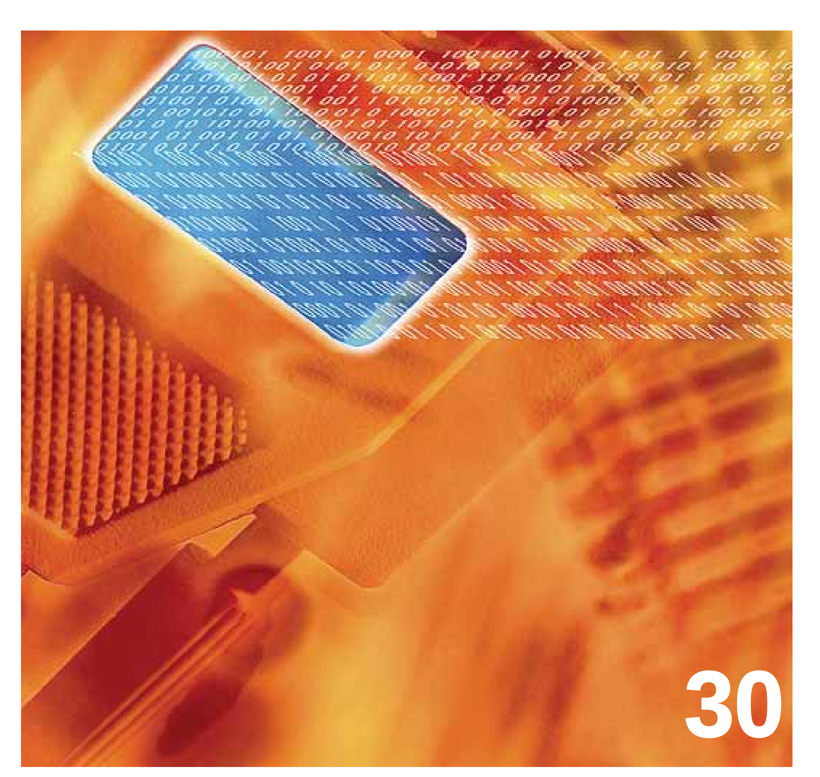
Reduce Fast Fast! SQL 2005

Reducir la silueta para exponer menos superficie de ataque. Ahí esta el secreto.



HARDWARE: PyMEs

Veremos dos propuestas de cómo una Pyme puede reducir sustancialmente la inversión destinada a un servidor, aprovechando la gran velocidad de las PC de escritorio disponibles hoy en día.



Seguridad en Linux Nota 2

En esta segunda nota veremos algunas de las condiciones necesarias y suficientes que nos permitirán plantear un buen esquema de defensa, ya sea de nuestra propia máquina como de toda una red.

Congreso Mundial 3GSM 2006



El 13 de Febrero abrió sus puertas la edición 2006 del **3GSM World Congress** que tuvo lugar, por primera vez, en el recinto ferial de Montjuïc de Fira de Barcelona.

La asistencia al congreso durante su primer día, superó a la de todo el evento de 2005. Los 50.000 participantes que asistieron este año, confirman que se trata del evento de telefonía móvil más grande del mundo.

Durante 4 días las principales operadoras telefónicas del mundo se congregaron para mostrar cuales fueron sus éxitos durante el año pasado y cuáles creen que lo serán en los años futuros. La industria de las comunicaciones móviles está cambiando hasta transformarse en una plataforma de distribución para el mundo del entretenimiento.

Motorola y Yahoo!, demostraron el uso de Yahoo! Podcasts en un dispositivo móvil. Por su parte, Steve Ballmer, CEO de Microsoft, y otros ejecutivos de la compañía, revelaron un nuevo servicio de televisión para teléfonos móviles y la pronta disponibilidad de Microsoft Office Communicator Mobile. Windows Live también hizo su debut durante estas presentaciones. Para más información sobre las tecnologías y novedades presentadas durante el congreso: *3gsmworldcongress.com*



RSA Conference 2006

Desde el 13 al 17 de Febrero, tuvo lugar en San Jose, California, la **RSA Conference 2006**, en la que se reunieron los directivos más influyentes de los principales mercados.

En su décimo quinto año el evento de seguridad y criptografía más importante del mundo atrajo a representantes del sector educativo, financiero, gubernamental, de networking, como también a Wall Street y a los medios.

Los asistentes pudieron disfrutar de prestigiosos oradores como **Bill Gates, Scott McNealy**, (Chairman y CEO de Sun Microsystems), **John Chambers**, (presidente y CEO de Cisco Systems), entre otros.

Los más de 14.000 profesionales de la seguridad que visitaron la conferencia durante sus 5 cinco días de duración, encontraron una inmensa cantidad de actividades como el **Executive Security Action Forum** (*ESAF*), el **Interactive Testing Challenge** (*ITC*), entre otras.

Por noveno año, se entregaron los **RSA Conference 2006 Awards** premiando las innovaciones en los rubros relacionados con las Matemáticas, Políticas Públicas y Prácticas de Seguridad. **RSA Security** es una reconocida empresa de seguridad informática desarrolladora del celebre algoritmo de encriptación RSA (Por sus autores: Ron **R**ivest, Adi **S**hamir y Len **A**dleman) y es la organizadora de esta conferencia desde su inicio en 1992.

CALENDARIO DE EVENTOS IT EN ARGENTINA PARA EL 2006

Fecha	MARZO	Informes
15	**Segurinfo 2006 -** Sheraton Libertador.	www.segurinfo.org.ar
20	**"Workshop in New and Emerging Technologies: Innovations in Communcations, Networks and VLSI" -** Hotel NH City (Bolívar 160)	Inscripción: ieeeuns@uns.edu.ar
	ABRIL	
-	**Jornadas Trabajo IT -** Sheraton Buenos Aires	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	JUNIO	
8	**Jornadas Trabajo IT Córdoba -** Córdoba Capital.	www.worktec.com.ar
9	**CIASFI Córdoba -** Córdoba Capital.	info@worktec.com.ar
22	**1er Jornada Nacional de Calidad en Software -** Sheraton Libertador.	Tel.:4511.3300
	SEPTIEMBRE	
19 y 20	**Consecri-Consetic 2006 -** Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	OCTUBRE	
3 al 6	**EXPO COMM -** La Rural, Predio Ferial de Buenos Aires.	www.expocomm.com.ar
6 y 7	**2do Congreso Nacional de Estudiantes de Sistemas y Tecnología de la Información. -** Lugar a confirmar.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300
	NOVIEMBRE	
2 al 5	**AES - Argentina Electronic Show -** La Rural, Predio Ferial de Buenos Aires.	http://www.aeshow.com.ar/es_services_contact_us
19 y 20	**Jornadas Trabajo IT 2 -** Sheraton Libertador.	www.worktec.com.ar - info@worktec.com.ar Tel.:4511.3300

Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar



"Securizar es la base"

Silvia Fandiño - IT Manager - **Organon Argentina**.

El propósito de esta serie de artículos es conocer soluciones propuestas por los profesionales de IT, pero también saber quienes son. En esta oportunidad NEX IT Specialist entrevista a Silvia Fandiño, IT Manager de Organon Argentina.

NEX: ¿Antes que nada podrías presentarnos a Silvia Fandiño? (perfil, estudios, intereses)
SF: Perfil tecnológico e innovador por supuesto, soy Ingeniera en Sistemas , graduada en la Universidad Tecnológica Nacional, posgrado en Dirección de Sistemas de Información (UB), Master en Business Administration (UTN) , me interesa profundamente adecuar los cambios y soluciones tecnológicas a los diferentes entornos que se presenten logrando la mejor combinación en términos de racionalidad y valor agregado real.

NEX: ¿Qué es Organon Argentina?
SF: Organon es un líder mundial de especialidades medicinales innovadoras para ginecología, salud mental y anestesia, productos que contribuyen a la salud de las personas y su calidad de vida. Es una unidad de negocio de AKZO NOBEL. La empresa farmacéutica holandesa Organon, desarrolla, produce y vende productos farmacéuticos. Desde su fundación, en 1923, Organon ha puesto el mayor énfasis en el desarrollo de productos que constituyan nuevos avances en el campo farmacéutico. Y durante los 80 años de su existencia, Organon introdujo muchos de los productos más innovadores en el campo de la fertilidad, la anticoncepción, la menopausia, la depresión y la anestesia. Aquí, en Argentina, más de 60 profesionales altamente motivados y capacitados, representan a Organon.

NEX: ¿Cuánto depende Organon Argentina de su infraestructura IT, de las aplicaciones (por ejemplo CRM), de su infraestructura Web?
SF: Organon Argentina está totalmente informatizada, utilizando a pleno los recursos que hoy por hoy están disponibles en el mercado, en términos de hard y soft, con usuarios altamente capacitados para la utilización de las herramientas disponibles. Estamos en pleno lanzamiento de Xlence, la nueva concepción de CRM para Organon Internacional (lanzamiento 2007).

NEX: ¿Por qué es importante gerenciar la seguridad informática en todos sus aspectos?
SF: El foco debe estar sin duda en este punto, ya que como CIOs uno de los objetivos y responsabilidades más obvias es proteger el patrimonio de las Compañías donde trabajamos. Hoy por hoy, aunque no sea tan evidente para los no informativos, las compañías están cada vez más expuestas a los ataques externos e internos (éstos cada vez menos frecuentes pero más efectivos), con alta diversidad de focos que requieren un efectivo gerenciamiento además de un fuerte know how en cada uno de los aspectos. Securizar es la base.

NEX: ¿Qué se ha hecho en este sentido? ¿Cuál es la integración con la red global de la empresa?
SF: Bastante. Primero analizamos estratégicamente los requerimientos del negocio, clasificando los procesos intervinientes. A partir de allí, diseñamos la solución requerida, que es una suite de antivirus centralizado, antispam, spyware a nivel desktop y montamos la LAN detrás de una solución robusta que combina hard, soft y soporte técnico muy efectivo. Todo administrado y controlado bajo IT con productos Check Point y con soporte externo de uno de sus partners Gold.

NEX: IT y la mujer. En NEX #22 (pág. 50) publicamos un estudio realizado por la prestigiosa revista windows IT Pro (www.windowsitpro.com) donde aparecía que el mundo profesional IT estaba conformado por sólo un 11% de mujeres. ¿Podés darnos tu visón de la mujer en IT y en particular en Argentina?
SF: Creo que es un mito decir que en IT hoy en día son todos hombres: la verdad es que en las otras profesiones también lo es... Ahora seriamente, en nuestro caso somos mayoría (2 mujeres y un hombre) y creo fehacientemente que la ingerencia de las mujeres en IT es muy fuerte, así como su performance, sobre todo en las áreas relacionadas con la Seguridad.

NEX: ¿Es grande el grupo IT local? ¿Podrías describir que tareas realizan y cuales se tercerizan?
SF: Somos una estructura pequeña de 3 personas: administrador de red, analista programador y IT manager, dando servicios de networking, training, ERP, CRM, SCM, help desk , asesoria y soporte a compañías del grupo (AKZO NOBEL CHEMICALS) y Organon Uruguay y además efectuamos desarrollo de aplicaciones en .NET (ASP y VB). Tercerizamos servicios de soporte técnico.

NEX: ¿Incidente de seguridad para comentar?
SF: My gosh! Tuvimos un ataque interno, de un ex empleado amateur, cuyo perfil era letal, del estilo "voy a probar lo que leí en el diario sección Informática a ver que pasa..." Lo cierto es que comenzó a probar vía webmail distintas claves de acceso que por ese entonces no eran de las que me gustan (tipo 52 caracteres, sin repetición) y logró entrar a una cuenta. Por supuesto, fue el fin de la historia, pero para ser honestos lo logró. ■

How would you like him poking around in your company's data?



Check Point Integrity protege a las empresas de los spywares

La solución de seguridad Nro 1 del mundo para los llamados "endpoint" (último punto en redes empresariales), Check Point IntegrityTM, protege a las empresas de los daños financieros causados por este tipo de ataque cuando los spywares abren backdoors, roban o exponen datos sensibles, reducen la performance de las PCs o incrementan los costos de las mesas de ayuda.

Aparte de neutralizarlos spywares, Integrity, provee la más completa y probada protección de los gusanos más recientes o las últimas técnicas de intrusión, para los "endpoints" empresariales y las redes a las que se conectan. Las defensas preventivas de IntegrityTM incluyen el firewall personal más confiable del mundo, bloqueos de amenazas outbound, prevención de intrusiones, remoción de spyware, y garantizan que sólo las PCs seguras tengan acceso a su red. De fácil implementación y administración Integrity se integra con más dispositivos de red que cualquier otra solución para proveer Protección Total de Acceso (Total Access Protection) para su empresa.

Con Integrity, le puede decir adiós al spyware y a tipos como éste.







Intelligent Security

For secure business evolution



Con los cambios en el mundo de los negocios, la información comercial y su uso están evolucionando. Ahora más que nunca, las empresas de todo tamaño necesitan soluciones para su seguridad que les permitan llevar a cabo sus actividades comerciales en nuevas formas para ser más competitivas y rentables.

Tradicionalmente, las soluciones de Check Point se han implementado para proteger el perímetro de las redes, principalmente para separar y proteger la red interna del mundo externo, y para conectar a múltiples oficinas y usuarios en forma segura a través de Internet. Cuando se tienen empleados remotos, "interno" puede significar fuera del perímetro original de la empresa. También, con el uso creciente de información empresarial por parte de los socios a través de la red, el panorama de la seguridad se hace aún más complejo.

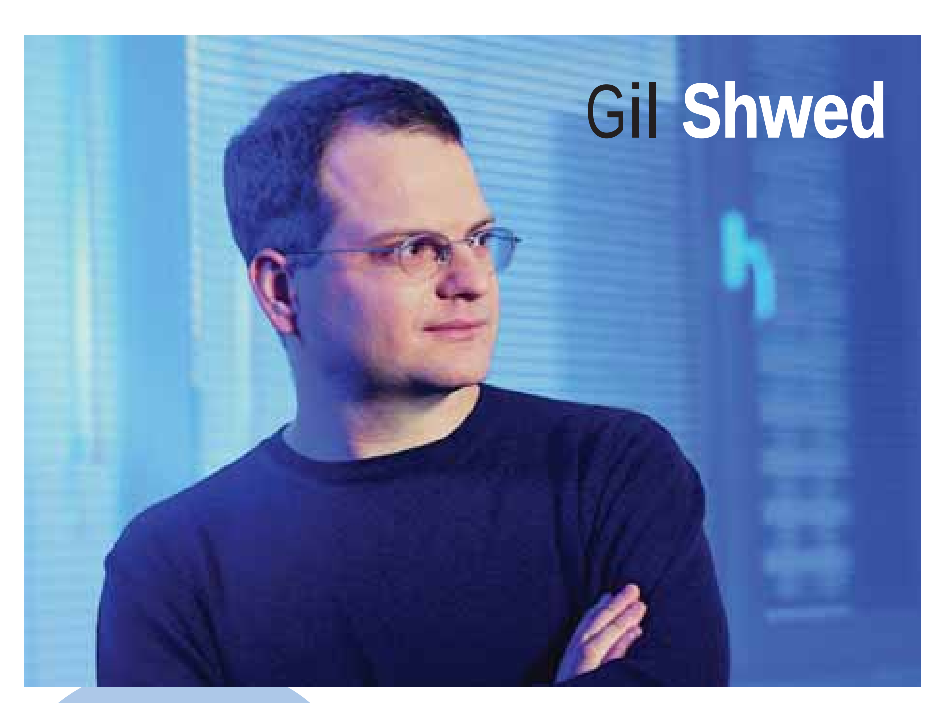
Nos hemos enfocado en una estrategia de seguridad perimetral, interna y Web para ampliar a lo largo y a lo ancho las soluciones que ofrece Check Point. Hemos potenciado nuestras tecnologías líderes del mercado para crear soluciones inteligentes para todas las organizaciones independientemente de su tamaño.

Con inteligencia, las soluciones Check Point aprenden fácilmente nuevos protocolos acerca de la forma como se comunican las aplicaciones. También detectan conductas sospechosas en la red que nunca han sido vistas y las detienen antes de que puedan causar daño.

Como mostramos en los siguientes artículos, nuestras nuevas soluciones inteligentes minimizan los riesgos, brindan un costo total de propiedad menor y ofrecen el más alto nivel de protección mientras permiten que los empleados, representantes y socios ingresen en forma segura. En pocas palabras, las soluciones inteligentes de Check Point preparan y refuerzan a las instituciones para competir y prosperar en un mundo en constantes cambios.

Gil Shwed - Fundador, Presidente y CEO

Historia y logros



Gil Shwed es Fundador, Chairman y CEO de Check Point Software Technologies, el líder mundial en seguridad de Internet. En 1993, Shwed inventó y patentó Statefull Inspection, que es hoy en día la tecnología estándar de los firewalls. Junto con los dos co-fundadores de Check Point, escribió la primer versión de FireWall-1, el producto emblema de la compañía que se convirtió en el primer firewall comercialmente disponible en 1994. En los años siguientes condujo a Check Point a ser el primero en ofrecer una solución de firewall integrado y VPN; Hoy la compañía es líder en ambos mercados de Firewall y VPN.

Con estas tecnologías revolucionarias como catalizadores, Shwed le dio vida a un nuevo segmento de mercado y rápidamente impulsó a su compañía hacia la cima de lo que es hoy la industria de la seguridad informática de miles de millones de dólares.

En 2003 Check Point redefinió el panorama de la seguridad de Internet bajo el liderazgo de Shwed con la presentación de la tecnología de Application Intelligence, un conjunto de capacidades avanzadas que detectan y previenen ataques a nivel de aplicación. Además, la compañía mantiene operaciones alrededor del mundo, y sus soluciones inteligentes perimetrales, internas y Web protegen cientos de miles de clientes, incluyendo al cien por ciento de las empresas listadas en Fortune 100.

Shwed ha recibido numerosos reconocimientos por sus logros individuales y contribuciones en la industria, incluyendo un Doctorado Honorario en Ciencias de Technion (Israel Institute of Technology) en 2004, nombrado Global Lider for Tomorrow por el World Economic Forum en 2003, por su compromiso con asuntos públicos y liderazgo en áreas más allá de los intereses inmediatos profesionales, y el premio Golden Plate de la Academy of Achievements por su contribución innovadora a los negocios y la tecnología, específicamente en el área de la seguridad de Internet y Networking (Junio de 2002).

La misión de Check Point

Hacer las comunicaciones en Internet seguras, confiables y disponibles en todos lados ha sido y continúa siendo su visión. Su compromiso es centrarse en las verdaderas necesidades de sus clientes, de modo de desarrollar nuevas e innovadoras soluciones de seguridad y seguir redefiniendo el panorama de la seguridad.

Su liderazgo en el Mercado:

- #1 a nivel mundial en software VPN/Firewall con un marketshare del 94% (Infonetics, Agosto 2005)
- Líder en Firewalls personales en "Personal Firewall Magic Quadrant" de Gartner (Gartner, 2005)
- #1 en el mundo en IPSec VPN/Firewall, con un 36% del mercado (Frost & Sullivan, Abril 2004).
- Líder en el mercado de IPSec VPN en el "IPSec Magic Quadrant" de Gartner (Gartner, 2000, 2001, 2002, 2004)
- Líder en el mercado de Enterprise Firewall y Network Intrusión Control, según "METAspectrum" de META Group (META Group - Marzo 2005).

Premios 2006:

- SC Magazine (USA): Best Enterprise Firewall por su producto VPN-1/FireWall-1 NGX, Mejor Remote Access VPN (IPSec) - Integrity SecureClient.
- MIS Best Choice Award - Institute for Information Industry - Best FireWall: Check Point VPN-1/FireWall-1 NGX , Best Broadband Internet Management Device VPN-1 Edge
- CRN Magazine - Febrero 2006: 2005 Channel Chiefs, 50 Local Leaders - Kevin Maloney.

Puede leer el listado completo de sus premios desde el año 2000 en: http://www.checkpoint.com/awards/index.html



Su Historia:

Check Point Software Technologies Ltd. (www.checkpoint.com), se dedica a asegurar la Internet desde su fundación en 1993 en Ramat-Gan, Israel, y cuentan actualmente con 1400 empleados. Su sede principal en Estados Unidos, se encuentra en Redwood City, California.
Es líder en el mercado mundial de firewalls corporativos y personales, y en VPNs. A través de su plataforma NGX, la empresa proporciona una arquitectura de seguridad unificada para un amplio rango de soluciones de seguridad (perimetrales, internas, Web, y endpoints) que protegen las comunicaciones de negocios y recursos para redes corporativas y aplicaciones, empleados remotos, sucursales y extranets. La línea de productos ZoneAlarm de la compañía, es la suite de seguridad para PC, mejor calificada, que cuenta con soluciones premiadas que protegen millones de PCs de hackers, spyware y robo de datos.
El poder de las soluciones de Check Point es extendida por su plataforma Open Platform Security (OPSEC), una alianza para la integración e interoperabilidad con soluciones que son las mejores de su clase, contando con más 350 compañías líderes. Cuenta con más de 2200 partners (canales) de distribución, y más de 350 OPSEC (Open Platform for Security) Partners. Entre sus clientes a nivel mundial tienen a más de 85 operadores telefónicos/ISPs, al 100% de las compañías del la lista Fortune 100, al 98% de las incluidas en Fortune 500.
Las soluciones de Check Point son vendidas, integradas, y asistidas por una red de más de 2200 Certified Partners en 88 países.
Recientemente adquirió a Zone Labs y a Sourcefire (Desarrolladores del Snort).
Cotiza en el índice NASDAQ desde 1996 y durante el año 2005, registró una facturación de $579.4 millones de dólares.

OPSEC:

OPSEC (Open Platform for security) es el framework de seguridad, abierto y multi-vendor que usa la industria. Con más de 350 socios, OPSEC garantiza a sus clientes la más amplia elección de las mejores plataformas de desarrollos y aplicaciones integradas de su clase. Los productos que llevan el sello certificado de OPSEC, han sido testeados para garantizar su integración e interoperabilidad.

"La mayoría de la gente cree que la seguridad es un factor limitante o un elemento negativo en sus planes de negocio. De hecho, una vez que la seguridad se vuelve algo que apoya sus negocios, se transforma en un verdadero empuje, que proporciona la confianza necesaria para llevar a cabo más negocios en línea."

- Gil Shwed -

Innovaciones Tecnológicas:

Stateful Inspection:
Stateful Inspection, inventada y patentada por Check Point, es la tecnología de seguridad de redes que ya se convirtió en un estándar por defecto y está basada en la tecnología INSPECT. Provee inspección precisa y altamente eficiente del tráfico con monitoreo completo a nivel de aplicación para el mayor nivel de seguridad. Los clientes experimentan alta performance, escalabilidad, y la capacidad de soportar aplicaciones nuevas y personalizables más rápidamente que con arquitecturas anteriores.

Malicious Code Protector:
Malicious Code Protector ofrece una innovadora tecnología (patente pendiente), que captura los ataques de buffer overflow y otros códigos maliciosos, permitiendo el mayor nivel de protección de la seguridad para clientes monitoreando las comunicaciones Web en busca de código ejecutable potencialmente malicioso.

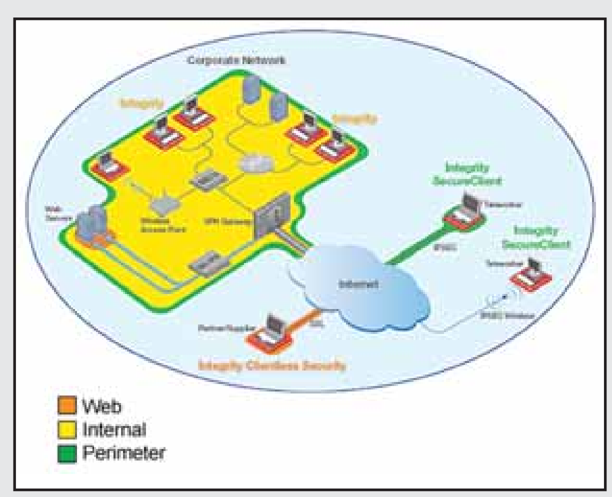
Application Intelligence:
Application Intelligence es un conjunto de capacidades avanzadas, integradas al Check Point FireWall-1 NG y SmartDefense, el cual detecta y previene ataques a nivel de aplicación. Application Intelligence está basado en INSPECT, y redefine el panorama de la seguridad de redes transformando al FireWall-1 en la única solución de seguridad que integra capacidades de protección tanto a nivel de red como de aplicación, para asegurar las redes y brindar una protección exhaustiva contra a ataques.

SMART Management (Security Management Architecture):
SMART Management pone a disposición un gran conjunto de sofisticadas capacidades administrativas en las soluciones Check Point. Su arquitectura está diseñada como una infraestructura de administración orientada a objetos, y le da a la industria capacidades de drag-and-drop que aseguran facilidad y escalabilidad de la administración. Comenzando con componentes centrales, como ser el Integrated Digital Certificate Authority y capacidades avanzadas de sincronización de tablas de estado, las tecnologías de SMART Management permiten a Check Point ofrecer herramientas de trabajo para satisfacer las necesidades de todas las organizaciones, desde servidores de Pymes hasta empresas de mayor tamaño e incluso proveedores de servicios globales.

Secure XL:
Secure XL es un framework de interfaces, módulos de software y estándares industriales que permiten a los socios y clientes de Check Point, montar soluciones al mejor costo para satisfacer los más exigentes requerimientos de performance. El Framework de SecureXL, junto con el compromiso de Check Point con los sistemas abiertos, ofrece una performance líder en la industria al más bajo costo posible.

TAP:
Los worms de rápida distribución, spyware cada vez más sofisticado, y otros ataques de hackers han causado enormes daños financieros a las empresas, a pesar del uso universal de antivirus. Claramente, es necesario un nuevo enfoque para detener los exploits a los end-points. La estrategia de Check Point para proteger los recursos de la empresa asegurando cada PC que se conecta a la red empresarial, se llama Total Access Protection. TAP se asegura de que todos los tipos de end-points, de empleados e invitados, remotos e internos, cableadas e inalámbricas, estén resguardadas por la mejor seguridad para endpoints. TAP también pone en cuarentena a PCs que no cumplen con las políticas de seguridad, previniendo que se conecten a la red hasta que cumplan con los requisitos de seguridad. Esta solución integral de seguridad, mantiene la disponibilidad de la red, previene el robo o exposición de datos sensibles, y protege las relaciones entre la empresa y sus clientes, y su preciada reputación.

TAP se implementa a través "Check Point Integrity", la galardonada línea de productos de seguridad para end-points. En conjunto, estas soluciones prestan protección preventiva para las PCs que se conectan a la red de la empresa a través de su perímetro, LAN, y servicios basados en la Web. Aseguran tanto las PCs propiedad de la empresa, como así también las de los clientes, contratistas, y otros socios de negocios que se conectan a los recursos IT de la empresa. Al integrarse con los Gateways de red de Check Point, sus socios OPSEC, y muchos otros vendors, Integrity puede reforzar los requerimientos de las políticas de seguridad, como ser tener actualizado el antivirus y parches, versiones específicas de programas y entradas de registro, y no tener programas prohibidos instalados. Integrity también permite a los administradores otorgar acceso limitado a la red a usuarios finales en los que no se se tiene confianza.



Total Access Protection *permite a las empresas defender todas sus PCs conectadas a la red, independientemente de su ubicación, propietario, o método de conexión.*

El ataque de los Zombies

Todos conocemos los Zombies, como lentas criaturas medio muertas, medio vivas, que persiguen sus victimas incesantemente, causando el terror y pánico. Hace años que los vimos en las películas y nos reímos, pues teniendo en cuenta su incapacidad atlética, sabemos que por mucho que la victima corra y el Zombie camine, en el final éste siempre la atrapa.

Su versión digital, no siendo tan conocida, es seguramente mucho más terrorífica.

Pedro Paixao
SE Manager (Security Expert Manager) Check Point

La creación de Zombies cibernéticos está intrínsecamente ligada a la creación de virus, gusanos (worms) y SPAM. En el inicio los virus eran transmitidos vía discos flexibles e infectaban millares de computadoras, a velocidades que hoy se pueden comparar a una tortuga. Después llegó la Internet y de miles pasamos rápidamente a millones de computadoras infectadas en pocas horas. De cara a este nuevo medio de distribución, los virus empezaron a ceder su lugar a gusanos, que al contrario de sus predecesores pueden replicarse automáticamente de computadora en computadora, sin intervención alguna. Aunque algunos de ellos sean extremadamente nocivos, podríamos así mismo considerar que su impacto es relativamente pequeño en lo que respecta nuestras vidas off-line. Quiero con esto decir que a pesar que un virus pueda formatear mi disco duro, no podía por ejemplo robar todo el dinero que tengo en el banco. Desafortunadamente la realidad de hoy es bien distinta.

Con la entrada del crimen organizado en la creación de virus, gusanos y SPAM de meras inconveniencias técnicas pasamos a crímenes reales que defraudan millones de personas y que suman millares de millones de dólares anualmente.

Tomemos como ejemplo el SPAM. ¿Puede que alguien compre Viagra a través de un mensaje de SPAM? La respuesta, por increíble que parezca es sí. ¡Estimativas apuntan a que aproximadamente un décimo de 1%, de personas que reciben SPAM contesta al mensaje o compra el producto!

Es fácil llegar a la conclusión que si se envían millones de mensajes rápidamente se acumulan las ganancias. Si un Spammer promociona un producto que le obtenga una ganancia de $50 pesos, significa que por cada millón de mensajes el va recibir 1000 pedidos, o sea una ganancia de $50,000 pesos. Desafortunadamente para nosotros, los usuarios, la dificultad de enviar mil millones de mensajes es la misma que enviar un millón, lo que representa la increíble suma de $50 millones de ganancias en el bolsillo del Spammer. ¡Queda claro entonces porque hoy más de la mitad del tráfico en Internet es SPAM!

Esta realidad fue expuesta por primera vez en los medios en 2004, en uno de los primeros casos de prisión de un Spammer. Jeremy James de 28 años vivía en una casa millonaria, era dueño de un restaurante de lujo y de una cadena de gimnasios, un resultado bien real de su profesión virtual. Jeremy recibía un promedio de $750 mil dólares al mes trabajando desde su casa, coordinando el envío de miles de millones de mensajes de correo electrónico.

El problema, para el Spammer claro, está en que una vez detectados, los sites de SPAM son rápidamente puestos abajo o bloqueados, con la posibilidad de prisión para sus dueños. Por otro lado, la capacidad de procesamiento y ancho de banda necesario para enviar tantos mensajes de correo representan una inversión que muchos no están dispuestos a pagar. La solución es enviar SPAM a través de una red de computadoras distribuida, pues maximiza las ganancias, minimiza la inversión y claro, el riesgo de captura y bloqueo.

Los riesgos para el Spammer son rápidamente minimizados cuando esta red sea compuesta por millares de usuarios y sus PCs hogareños. Llegamos así a las razones por las cuales existe un claro incentivo monetario para la creación de virus, gusanos, u otros tipos de spyware.

Aprovechando vulnerabilidades existentes en aplicaciones de uso común, como el Internet Explorer, Messenger, Skype, etc. el criminal puede tomar el control de miles de computadoras, y transformarlas en Zombies. A partir del momento de la infección, el Zombie pasa a obedecer a las órdenes recibidas, normalmente vía Internet Relay Chat o IRC. El atacante envía el virus o gusano unas cuantas veces y después espera que los Zombies empiecen a reportar por miles en el chat room designado. Cuando desea que los Zombies ejecuten una orden, solo tiene que entrar al chat y enviar el comando apropiado. Una vez recibida la orden los Zombies reaccionan de manera automática y masiva.

En una red de Zombies grupos de PCs infectados envían mensajes durante períodos cortos y después paran, pasando la estafeta al próximo grupo. Este método evita la detección por parte del usuario y su ISP. Todos estamos acostumbrados a períodos de mal desempeño de nuestra PC: durante breves momentos el Windows escribe en el disco incesantemente, al tiempo para, y nada funciona,



hasta parece que entramos en el Triangulo de las Bermudas. Estamos tan acostumbrados que ya ni frustración sentimos con lo sucedido: paramos un poco, tomamos un café, o aprovechamos para conversar con el compañero del lado. No nos pasa por la cabeza que la razón detrás de tal problema pueda ser el hecho que nuestra PC es en la realidad un Zombie atacando millares de potenciales victimas en Internet

En Junio de 2004 los sites de Microsoft, CNN, y Yahoo, entre otros; desaparecieron por completo de Internet durante horas. En esta situación una red de Zombies con aproximadamente 60 mil computadoras fue utilizada para generar miles de pedidos por segundo a cada uno de los servidores, que quedaron completamente incapacitados.

En Enero de 2006, durante su juicio, un hacker Californiano se declaró culpable por mantener una red de 400,000 Zombies, la cual el "rentaba" a Spammers y publicidad tipo "Pop-up", por millares de dólares.

Tal vez el punto mas importante no sea el hecho de que el individuo fue capturado, sino el crecimiento que las redes de Zombies presentaron en cerca de un año. En 2004 el estado de la situación se aproximaba a los 60,000 Zombies, para 2005 ya vamos en 400,000. Un crecimiento de más de 600%. Éste es un problema sin fronteras que afecta cualquier computadora conectada con Internet. Según varios estudios de empresas especializadas como CipherTrust e ICSA, el número de Zombies está en crecimiento exponencial siendo que México cuenta con aproximadamente 3% de los Zombies mundiales.

Para que estas redes de Zombies funcionen son necesarias direcciones de correo electrónico. Sin ellas no hay a quien enviar el SPAM. Aquí entra en acción otra clase de individuo cuyo trabajo es colectar millones de direcciones de correo en Internet. Utilizan todo desde páginas web, grupos de noticias, grupos de discusión, comunidades… En fin, cualquier cosa que tenga parecido con un correo electrónico y que esté publicado en Internet, será capturado.

Después crean listas que se venden alrededor de $5 dólares por cada millón de direcciones. Sin embargo éstas son listas de bajo valor para el verdadero Spammer, pues están llenas de direcciones inválidas, u obsoletas, y "peor" que todo, llenas de direcciones de empresas de Anti-Spam que utilizan estas cuentas de correo para después identificar y bloquear el Spammer.

Por estas razones listas de direcciones válidas son vendidas en el mercado a precios exorbitantes. En Junio de 2004 autoridades Norteamericanas arrestaron un joven ingeniero de AOL por haber vendido 92 millones de direcciones de correo electrónico válidos por $100,000 dólares, o sea mas de $1000 dólares por cada millón de direcciones!

Podemos finalmente reconstruir el panorama completo: tenemos los creadores de virus y gusanos que permiten transformar una computadora en un Zombie, extrayendo de esas computadoras todo el tipo de información privada, que es vendida a compiladores de listas de correos electrónicos, tarjetas de crédito etc., que a la vez venden sus servicios a los Spammers, que utilizan los Zombies para enviar millones y millones de mensajes.

En el medio del panorama estamos todos nosotros, aun los que no tienen computadora, pues su información personal está almacenada en forma digital en algún sistema de gobierno o empresa con la cual mantenemos una relación profesional o de negocio.

El hecho de que estas actividades se transformaron en profesiones extremadamente lucrativas implica que ellas no van desaparecer en tiempos próximos, y que por ahora las soluciones legales para este problema no son detrimento suficiente.

Cabe a cada uno de nosotros hacer lo que está a nuestro alcance para minimizar esta invasión, aunque eso implique no abrir el correo de un amigo o amiga, con la última foto chistosa, no contestar a ningún mensaje de SPAM por increíble que sea el producto o negocio. Mantener el antivirus y anti-spyware actualizado sea en el gateway con Check Point Express CI o en el cliente con el firewall personal como Integrity o Zone Alarm.

Recuerde: Para el hacker la ganancia está en los grandes números, y para nosotros está en no ser parte de ellos!

Soluciones Check Point que mitigan estos ataques:

Check Point Express CI - Firewall, VPN, Antivirus, IPS en un solo gateway

Integrity Suite - Firewall personal, Antivirus, anti spyware, control de mensajería.

“Los ataques de buffer overflow en aplicaciones son hoy una de las peores y más devastadoras vulnerabilidades en Internet”

Malicious CODE PROTECTOR



Ataques que utilizan buffer overflows se han tornado uno de los mayores problemas de seguridad en Internet, siendo responsables por más del 50% de los reportes informativos de vulnerabilidades del CERT. El atractivo para este tipo de ataque es el poder controlar completa y remotamente la máquina vulnerable, y por lo cual algunos de los peores y mayores ataques en los últimos años se pueden atribuir a vulnerabilidades de buffer overflow.

A través de ataques de buffer overflow el hacker puede iniciar o terminar aplicaciones, borrar archivos, inyectar código suyo, instalar software malicioso, etc. Los gusanos son un buen ejemplo de cómo se puede utilizar una vulnerabilidad de buffer overflow para instalar código malicioso que se propaga por todo Internet en pocas horas.

Debido al tremendo impacto que estas vulnerabilidades pueden tener, se estima que sean cada vez más utilizadas en ataques futuros.

Algunos fabricantes desarrollaron tecnologías para intentar bloquear este tipo de ataques, pero las soluciones actuales son incapaces de identificar ataques desconocidos, o mismo variaciones de ataques conocidos. Éstos son problemas críticos, debido a la velocidad con que se propagan estos ataques. Para solucionar este problema Check Point desarrolló una nueva tecnología, de patente pendiente, con el nombre de Malicious Code Protector. Esta tecnología permite bloquear ataques de buffer overflow, sin depender de firmas, y pudiendo detectar ataques desconocidos.



Pedro Paixao
SE Manager (Security Expert Manager)
Check Point



En un mundo ideal las aplicaciones no aceptarían más datos que lo esperado por el desarrollador, y ningún sistema dejaría escribir fuera de un buffer de memoria previamente alocada. Sin embargo existen miles de aplicaciones que no verifican los datos de entrada, y millones de hosts las ejecutan en todo el mundo. La incapacidad de cambiar todas las aplicaciones utilizadas por una empresa, u organización, para que todos los puntos de entrada de datos sean respetados y validados, implica que se intente solucionar el problema a nivel de red, antes que se llegue a la aplicación. Los ataques de buffer overflow explotan aplicaciones, pero necesitan de la red para llegar a éstas.

Genéricamente las soluciones típicas para este problema se conocen como sistemas de detección de intrusos (IDS del inglés) o Sistemas de Protección de Intrusos (IPS). Los IDS intentan detectar ataques a aplicaciones, buscando patrones conocidos o anomalías, en los flujos de datos que pasan en la red. Si se encuentra un patrón conocido o se detecta tráfico "anormal" se avisa al administrador de red que un ataque está en curso, y normalmente no tienen la capacidad de bloquear los ataques detectados. Los IDS son sistemas de aviso y no protección. Las ventajas de estos sistemas es que normalmente no impactan al tráfico en la red directamente. Sus desventajas son que no pueden bloquear los ataques que detectan, y también su falta de mecanismos de identificación preventivos, no reactivos. Si no hay firma/patrón no hay detección. Como ejemplo se puede utilizar el CodeRed II. Este ataque solo tenía 13 bytes diferentes de su primera versión, pero infectaba a sus victimas 3 veces (cuadro 1) más rápido, y muchos IDS no pudieron detectar esta variación del original.

Debido a esta importante deficiencia, algunos fabricantes de sistemas IDS alegan tener la capacidad de inspeccionar código maquina (assembly), cuando en la realidad lo que hacen es buscar secuencias conocidas de bytes, que pueden inferir código máquina. Esta diferencia sutil hace que muchas veces no se detecte ataques desconocidos o variaciones de ataques conocidos.

Los sistemas IPS ya tienen la capacidad de bloquear ataques, eliminando una de las importantes desventajas que sus predecesores, los IDS, tenían. Sin embargo, como se basan en la misma tecnología que los IDS sufren también de la incapacidad o dificultad para detectar ataques nuevos.

El diseño del Malicious Code Protector (MCP) apunta a eliminar las desventajas de las tecnologías actuales, identificando código ejecu-

Ataque	Año	Impacto Económico	Vulnerabilidad
Sasser	2004	$3.5 mil millones	MS Local Security Authority
SQL Slammer	2003	$1 mil millones	Microsoft SQL Server
MS Blaster	2003	$750 millones	Microsoft RPC
Code Red	2001	$2.6 mil millones	Microsoft IIS

Cuado 1.



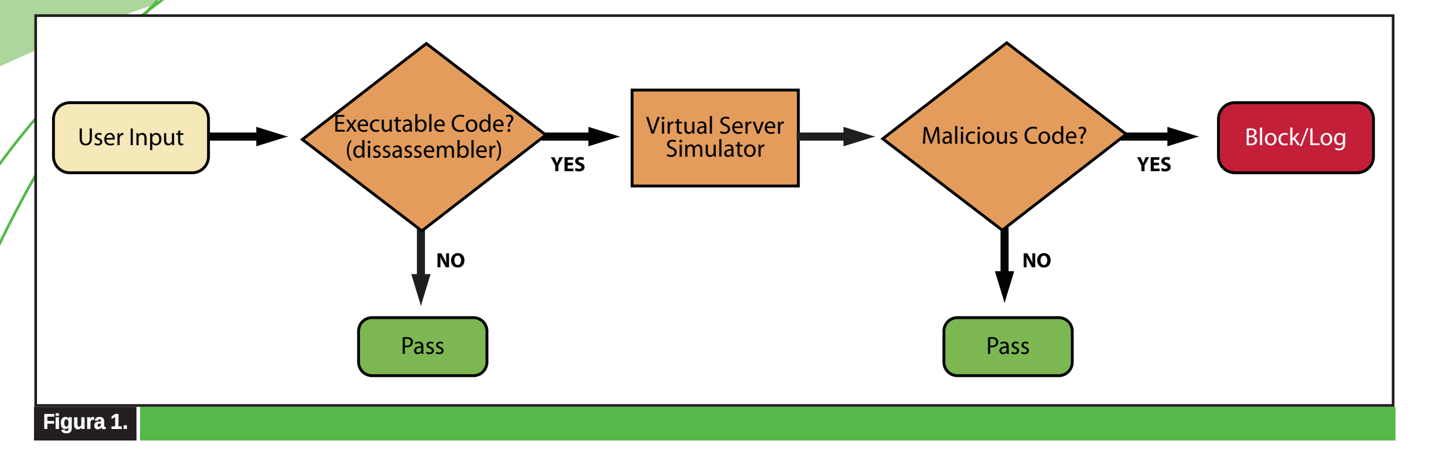


Figura 1.

table, interpretando sus instrucciones máquina, y bloqueando ataques sin recurso a firmas. Los objetivos de diseño del MCP son primariamente

1. Detección de ataques desconocidos. La base del MCP es detectar el ataque en sí, y no un patrón conocido del mismo ataque.
2. Independencia de protocolos. Haciendo parte de la infrastructura de Check Point Application Intelligence, el MCP soporta más de una docena de protocolos, como http, SQL, MS-RPC, etc.
3. Rapidez. Hacer todo el trabajo a más de 1 Gbps, en plataformas de hardware comunes.
4. Independencia de plataforma. Sabemos que 90% de los servidores en Internet utilizan plataformas x86, pero el 10% restante es igualmente importante desde el punto de vista de la seguridad, como tal el MCP soporta arquitecturas Intel o SPARC.

Se asumió también que todos los ataques de buffer overflow, de una manera u otra, envían código máquina que será ejecutado por la victima después de explotado el buffer overflow. Sin este código no se puede tomar el control de la victima. El "corazón" del MCP es el Disassembler que busca por código máquina en el tráfico de red. Una vez identificados los segmentos que pueden contener código máquina éstos son "desensamblados" y enviados a la maquina virtual (Virtual Server) que los interpreta. En el Virtual Server se identifica el comportamiento del código ejecutable y se analiza si éste es malicioso o no. Por ejemplo se analiza si se reescribe el Instruction Pointer del CPU. Si después del análisis se identifica un comportamiento malicioso del código se bloquea toda la sesión, y se genera un log.

Uno de los desafíos de todas las tecnologías que utilizan interpretación de código maquina es la de minimizar los falsos positivos, o sea tráfico "bueno" que se identifica como malicioso. Para hacer ésto, el MCP no se limita a interpretar el código máquina, el MCP reconstruye el flujo del código, identificando loops, condiciones (IF) y otros elementos lógicos de programación. Este abordaje permite identificar métodos conocidos de programación de vulnerabilidades y reducir la probabilidad de que secuencias aleatorias de código sean interpretadas como maliciosas.

Otro de los puntos importantes, mencionados anteriormente, es el desempeño. El MCP sólo se aplica en puntos del tráfico que pueden ser utilizados para introducción de datos, como por ejemplo campos de una forma web, o encabezado HTTP. De esta manera se optimiza la ejecución del sistema lo que permite el uso de esta tecnología en ambientes de alto rendimiento.

Al no utilizar firmas para detectar los ataques se consigue una solución preventiva que permite identificar ataques desconocidos o variaciones de ataques conocidos. Como ejemplo de ésto se bloquearon los gusanos, Code Red, y todas sus variaciones, Nimbda, Witty, SQL Slammer, en su primer día (zero day) sin actualización del producto.

El MCP esta incluido en varias soluciones de Check Point, como el VPN-1 NGX, el Connectra (VPN SSL) y Integrity (firewall personal Zone Alarm).

	Descripción	Datos
1	Ejemplo de un paquete con código malicioso	...FF 73 47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 6F 6F 6F 6F 6F 6F 6F 6F 6F 6F 6F 6F 42 42 42 42 8B 89 E8 77 EB 15 5B 53 68 AA 01 78 58 FF D0 31 C9 B1 11 58 E2 FD 31 C0 48 C3 E8 E6 FF FF FF 73 74 61 72 74 20 63 61 6C 63 2E 65 78 65 00 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A 0D 0A...
2	Con el conocimiento del protocolo http, el VPN-1 reconoce este flujo de datos como un comando HTTP GET	GET / HTTP/1.1Host: ooooooooooooBBBBïë_w_ [Sh¡ xX _1__ X__1_H__µ start calc.exe Connection: close
3	El MCP detecta el código ejecutable y interpreta sus instrucciones	JMP+26, CALL-26, POP EBX, PUSH EBX, PUSH 0x7801AAAD, POP EAX, CALL EAX
4	La máquina virtual del MCP ejecuta el código y determina que es malicioso	**BLOQUEAR SESION!**

Cuado 2.

Conclusiones

Los ataques de buffer overflow en aplicaciones son hoy una de las peores y más devastadoras vulnerabilidades en Internet, causando miles de millones de dólares de pérdidas todos los años. Debido a las tecnologías de protección existentes, como IDS e IPS, existe una ventana de vulnerabilidad que se mantiene abierta durante el período en que sale un ataque y los varios fabricantes publican una firma para su identificación y bloqueo. Esta ventana llega a ser de semanas dependiendo del ataque y su impacto. Durante este tiempo todos los sistemas vulnerables pueden ser victimizados y comprometidos. El Malicious Code Protector, al no utilizar firmas, e identificar código malicioso directamente, permite tener una solución preventiva que bloquea ataques desconocidos en su primer día. Esta capacidad, aliada a su elevado desempeño torna el MCP en la solución más avanzada de protección de buffer overflows del mercado.

"Necesito mantener la información segura, **en todo lugar.**"

"Necesito ayudar a mis pacientes, **desde cualquier lugar.**"

Check Point Connectra hace feliz a ambos con acceso desde cualquier lugar y seguridad en todo lugar.

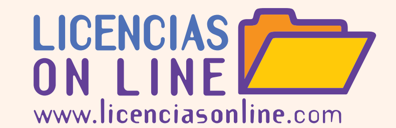
NGX

Mantener la información segura no tiene porque estar en contraposición con proveer acceso sencillo. Solo Check Point Connectra combina acceso SSL VPN desde cualquier Web-browser, asegura la transmisión de información sobre salud via SSL, y provee la inmunidad más potente contra spyware, gusanos y otros riesgos a la privacidad de datos.

Connectra es la receta correcta para acceso desde cualquier lugar y seguridad en todo lugar.

Conéctate hoy a www.licenciasonline.com para información sobre soluciones Connectra en salud.

Aprenda como usted puede hacer que los médicos estén contentos mientras mantiene la información segura a través del acceso remoto disponible más seguro y conveniente. Y descubra como Connectra provee los controles de seguridad que usted necesita de modo que pueda cumplir las regulaciones de HIPPA.





La SEGURIDAD comienza en NUESTRA CASA





Fernando Santos
Gerente de Área Cono Sur
Check Point



¿Cuál es el nuevo escenario que plantea la seguridad informática? ¿Qué es lo que se debe hacer? ¿Cuáles son los desafíos de seguridad para las empresas en 2006? Este artículo nos responde de estas preguntas y nos detalla cuatro consejos que pueden ayudar en esta gestión.

Imagine que usted fuese la persona responsable del gallinero de una chacra, y la seguridad está amenazada: zorros hambrientos están al acecho. En los últimos años su protección se basó en hacer la pared perimetral cada más alta y reforzarla. Ésto sirvió, pero ya no sirve más…

Pensemos ahora en un cuento mágico irreal, donde los zorros adquirieron superpoderes, obtuvieron alas y tienen la capacidad de excavar túneles por debajo de la tierra en busca de gallinas y huevos... más aún ahora pueden hasta usar disfraces de gallina.

Modificar la pared ya no es suficiente y los zorros tienen que ser detenidos. Pero aún más, ¿Qué pasa si los zorros con piel de gallina estuviesen ya instalados confortablemente dentro del gallinero?

La metáfora puede parecer alejada de la realidad de las empresas, sus *assets* y su seguridad, pero en verdad no lo está. En lugar de gallinas y huevos hablamos del patrimonio de las empresas, la red de datos donde transita la información y



empleados. La pared es el firewall de protección; los zorros, representan los virus, hackers o también potentes y sofisticados worms.
En 2005, las empresas pudieron ver como se desmoronaba la pared. Esto ha hecho que toda la industria de IT tuviera que reinventarse para atender problemas que hasta entonces no se habían manifestado: los ataques se sofisticaron y la red corporativa hace ya mucho transpuso las fronteras del firewall. Nuevos horizontes, redefinidos por tecnologias que cambiaron los conceptos de perímetro de red y tambien del "punto de trabajo". Los que antes parecían fijos e inmutables, ahora tienen alas y están más móviles y más flexibles que nunca.
La realidad es que los ataques cambiaron de categoría. Saltaron de la capa de red, donde el firewall estaba suficientemente bien para la detección, y migraron a la capa de aplicación. El tráfico legítimo es ahora utilizado por los ataques "enlatados". Por esto hubo el año pasado una escalada en la utilización de Sistemas de Deteccion y Prevensión de Intrusos (IDS e IDPs) para posibilitar la identificacion de ataques que parecian tráfico legítimo. Con esto, el firewall recibió el refuerzo de tecnologias que permiten averiguar como con Rayos X todo lo que entra en la red.
Otro cambio radical fue la aparición de un escenario donde los empleados usan toda la suerte de accesos wireless; celulares donde se pueden bajar correo; notebooks y handhelds con acceso a Internet. Todo esto en principio es bueno para la industria, representa comodidad para el usuario, pero también es una amenaza inminente a la red y la seguridad, particularmente cuando se mira el mar de worms, spywares, malwares, etc que están agazapados esperando la primera victima al ver que algunas gallinas resolvieron salir para dar un paseo fuera de los límites del gallinero.
¿Entonces qué es lo que se debe hacer en este nuevo escenario? ¿Cuales son los desafíos de seguridad para las empresas en 2006? Lo que puedo decir es que no hay fórmulas ya concebidas, cada compañía tiene que hacer los deberes en casa, evaluar sus vulnerabilidades. Hay, cuatro consejos que pueden ayudar en esta gestión:

- Mantenga siempre su gateway y firewall actualizados. En el día-a-día, equivale a estructurar un sistema capaz de detectar y prever ataques hacia la empresa, cuyo origen es fundamentalmente Internet. Teniéndose en cuenta que el correo electrónico es hoy la principal herramienta de comunicación, un firewall bien configurado, fortalecido con un IDS puede traer un buen nivel de protección a la puerta de entrada de la compañía. Adicionase a esto el antivirus para el gateway y correo para no tener problemas de virus de correo y ya tenemos la seguridad perimetral satisfactoriamente implementada con un buen nivel de seguridad.
- Especial atención a la seguridad interna, independientemente de su firewall. Y teniendo en cuenta que la mayor parte de las vulnerabilidades se ubican adentro de las empresas, y no afuera de ellas, procuremos minimizar el riesgo segmentando la red y los accesos. Un modo eficiente es el de definir los accesos de los usuarios solamente a los datos y servidores que necesitan acceder para hacer su trabajo, nada más. Hay también sistemas que hacen divisiones de la red en zonas de seguridad compartimentadas. En otras palabras, redes más chicas dentro de una más grande. Se pueden tener firewalls internos estratégicamente posicionados por departamentos y en el momento del ataque evitar que toda la red o personas se contaminen o queden expuestas.
- Impedir que el punto de acceso del usuario sea contaminado. Ésto incluye desde la educación (que no se abran correos cuyo origen no se conoce), hasta herramientas de control y seguridad, como firewall personal que contiene el antivirus, el antispyware, antiworms, etc. En este punto, también, hay mucho trabajo por hacer: desde una mirada criteriosa en la utilización que sus usuarios hacen de la red y su recursos, hasta medidas de protección de nuevas tecnologías como VoIP, wireless, Skype, Instant Messaging, y otras.
- Cuidado con su sitio web, principalmente si ésta es una herramienta importante para los negocios. Ataques específicos a las herramientas Web han se tornado muy comunes y la tarea de garantizar protección se ha hecho más difícil ya que es necesario realizar una seguridad específica para el tráfico Web para proteger no sólo el sitio sino también las aplicaciones de B2B, B2C y acceso SSL VPN. ■

http://www.checkpoint.com/form/promo/2006LatinAmericaConnectraIntegrityAdvertising-SSL-SP.html

SECCIÓN ESPECIAL



¿Su seguridad pasará la prueba del tiempo?

Por qué puede contar con las **soluciones** de **Check Point**

Cuando se trata de proteger su empresa, entendemos lo importante que es su confianza. La mejor tecnología tiene que estar respaldada por una compañía confiable. Por eso debe saber las siguientes cosas acerca de Check Point.

La seguridad es nuestro único negocio. No es una idea nuestra de último momento. Nuestro objetivo nunca se desvía de nuestra principal preocupación: proporcionar las soluciones de seguridad que permitan a nuestros clientes tener éxito.

Su empresa está en las manos más seguras con Check Point. Es una responsabilidad que aceptamos seriamente.

Somos innovadores. Otros nos siguen a donde vamos. Cuando usted elige las soluciones de Check Point, obtiene Stateful Inspection, la norma reconocida en la industria para firewalls creada por los expertos. Nosotros la inventamos. Nuestra tecnología ha sido imitada, pero nunca igualada. La tecnología INSPECT de Check Point observa más profundamente el tráfico, y lo mejor de todo es que aprende fácilmente nuevos protocolos para comunicaciones de voz, video y datos. INSPECT es la base de muchos otros hitos de Check Point. Por ejemplo, fuimos los primeros en integrar seguridad a nivel de red y a nivel de aplicaciones en una solución única para una seguridad más amplia. También tenemos una patente en trámite para Malicious Code Protector™, un elemento de nuestra tecnología de Web Intelligence que burla los ataques al detectar y bloquear nuevos tipos de amenazas de Internet. Además, somos el único fabricante de seguridad con administración constante integrada en toda la infraestructura de seguridad.



Hemos estado en el negocio de las soluciones de seguridad durante 12 años. Durante ese tiempo, un gran número de compañías con soluciones rápidas a problemas limitados han pasado. Nuestra longevidad se debe a nuestro enfoque en soluciones de largo plazo. La tecnología que inventamos para la seguridad perimetral es igualmente aplicable y eficaz para la seguridad interna y Web, que son esenciales para las nuevas modalidades comerciales.

Con el transcurso de los años, nuestras tecnologías básicas han madurado y demostrado lo que son en los entornos más exigentes de centros de datos empresariales y proveedores de servicio. El cien por ciento de las 100 compañías de mayor tamaño de Fortune confían en las soluciones de Check Point. Lo mismo ocurre con miles de compañías pequeñas.

Mediante nuestra estrategia de canales, hemos formado un grupo amplio en el mundo entero con los mejores expertos en seguridad. Las soluciones de Check Point son vendidas, integradas y atendidas por una red de más de 2,200 socios certificados de Check Point en 88 países. Establecimos OPSEC (Open Platform for Security), primera arquitectura abierta de seguridad, de modo que los fabricantes pudieran desarrollar productos que funcionen con nuestras soluciones. Cientos de compañías certifican sus aplicaciones y plataformas para integrarse con la seguridad de Check Point.

Nuestra longevidad se debe a nuestro enfoque en **soluciones de largo plazo**.

Creemos que estos hechos respaldan nuestra conclusión. Su empresa está en las manos más seguras con Check Point. Es una responsabilidad que aceptamos seriamente.

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.



A la vanguardia de la **evolución en seguridad**:

Check Point es la primera empresa en ofrecer una solución acertada e inteligente tras otra.

Stateful Inspection
Patentada por Check Point para inspección precisa y altamente eficaz de tráfico.

SMART
Capacidades administrativas sofisticadas para todas las organizaciones, desde empresas pequeñas hasta empresas mayores expandidas y proveedores mundiales de servicios.

OPSEC (Open Platform for Security)
La primera arquitectura de seguridad abierta. Cientos de socios OPSEC brindan a los clientes las más amplias opciones y plataformas de implementación.

SecureXL
Estructura de interfaces, módulos de software y estándares industriales para conformar soluciones para los requisitos de desempeño más exigentes.

Application Intelligence
Integra capacidades a nivel de red y de aplicación para ofrecer una protección amplia contra ataques y seguridad de redes.

Web Intelligence
Inspecciona el contenido Web y el código de aplicación y actúa en forma preventiva contra los ataques.

Malicious Code Protector
Tecnología de patente en trámite que detecta y bloquea incluso ataques de desbordamiento de buffer previamente desconocidos.



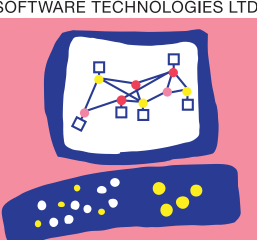
Nuestros **Clientes**

Hemos ayudado a empresas grandes y pequeñas a cambiar su forma de pensar acerca de la seguridad. Éstos son algunos de los datos estadísticos de clientes de los que estamos orgullosos:

- 100% de las 100 compañías más grandes de Fortune
- 97% de las 500 compañías más grandes de Fortune
- 99% de las 100 compañías más grandes de Global
- 96% de las 500 compañías más grandes de Global



Check Point SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Check Point
Security Tour 2006

Creando una Agenda de Seguridad para el Crecimiento

Su negocio continúa expandiéndose y usted es responsable de instalar nuevas oficinas, empleados y aplicaciones a una ya extralimitada infraestructura de red. De alguna manera, usted necesita administrar su crecimiento manteniendo a la vez una fuerte postura de seguridad. Unirse al Check Point Security Tour le permitirá conocer la mejor protección contra nuevas amenazas, teniendo así la clave para que su compañía mantenga un crecimiento ilimitado.

También aprenderá cómo:

- Incrementar la efectividad de su creciente número de usuarios móviles permitiendo acceso seguro y sin restricciones a diversas aplicaciones

- Expandir de manera segura su red hacia oficinas remotas en todo el mundo sin comprometer su seguridad o aumentar costos de administración

- Habilitar a sus empleados, socios y otros usuarios el acceso a recursos de la red mientras previene gusanos y spyware

- Utilizar tecnología VoIP para reducir los costos de comunicación de voz sin sacrificar la seguridad

México D.F. 16 de Marzo, 2006. Club France
Av. Francia No. 75. Col Florida. México D.F.

Proximamente en Argentina

8:00 a.m. - 8:30 a.m.	Coffee – Registro
8:30 a.m. - 8:45 a.m.	Bienvenida Check Point
8:45 a.m. - 9:30 a.m.	Las 10 Mejores Maneras de Proteger a Usuarios Remotos
9:30 a.m. - 10:00 a.m.	¿Abierto a los Negocios? Estrategias para abrir de manera segura sus nuevas oficinas
10:30 a.m. - 10:45 a.m.	Una guía sobre cómo proveer acceso seguro a la red para cada usuario
10:45 a.m. - 11:30 a.m.	Coffee Break
11:30 a.m. - 11:45 a.m.	Las mejores prácticas para utilizar VoIP de manera segura
11:45 a.m. - 12:30 a.m.	Demostraciones de productos
12:30 a.m. - 13:00 a.m.	Cómo gerenciar la seguridad de manera sencilla
13:00 a.m. - 13:30 p.m.	Los siguientes pasos para el crecimiento de su negocio
13:30 p.m. - 14:45 p.m.	Almuerzo
14:45 p.m. - 15:30 p.m.	Crossbeam - Gestión Unificada de Amenazas: la Nueva Generación de Seguridad
15:30 p.m. - 16:15 p.m.	Websense
16:15 p.m. - 16:30 p.m.	Coffee break
16:30 p.m. - 16:50 p.m.	Aladdin
16:50 p.m. - 17:35 p.m.	Nokia
17:35 p.m. - 17:35 p.m.	Radware

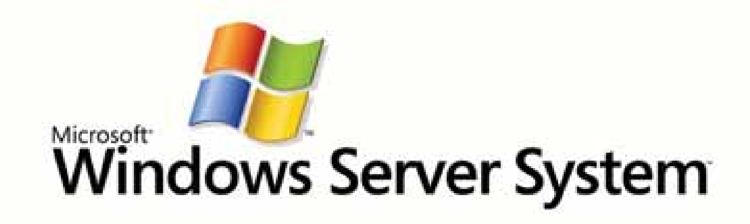
Microsoft

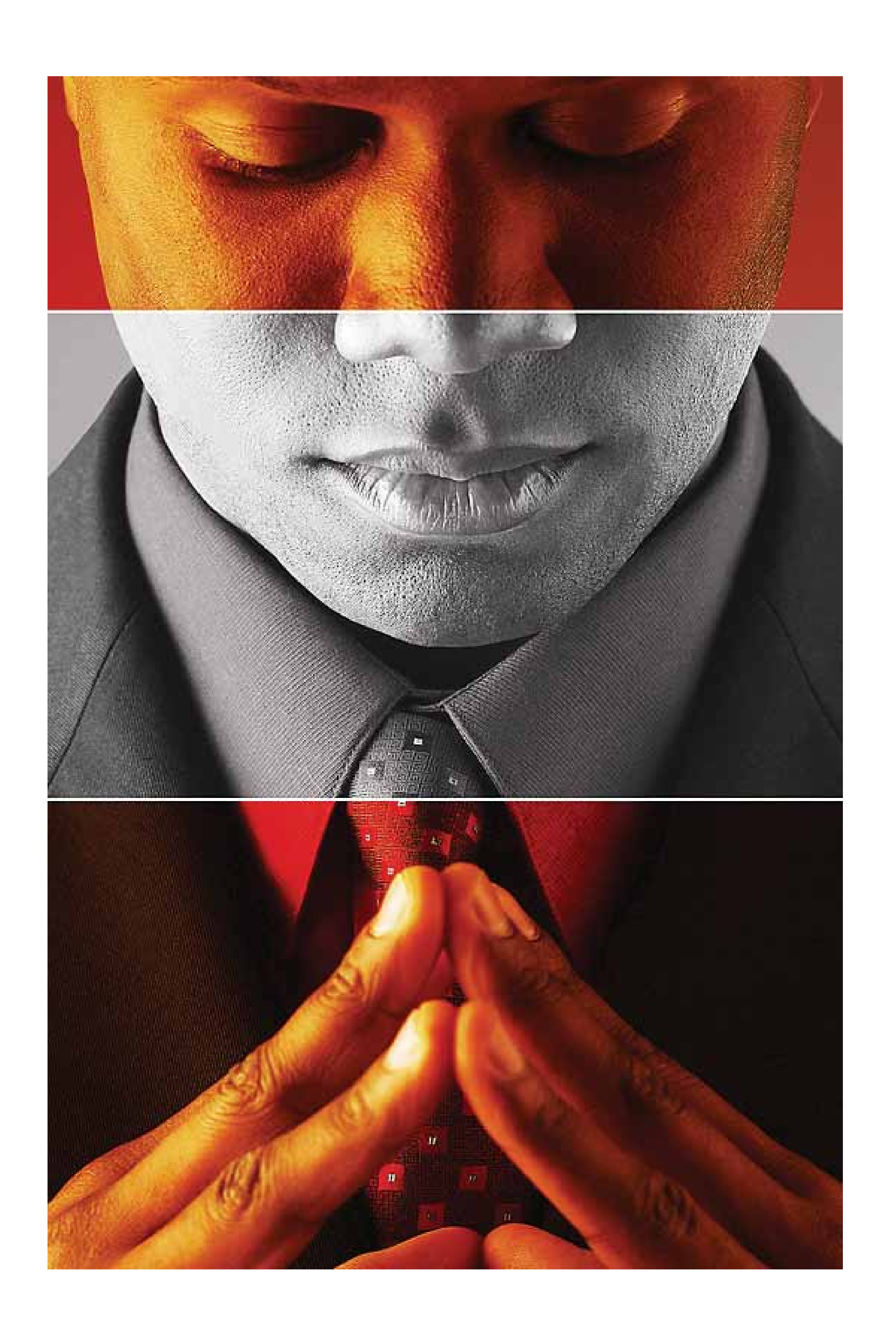
Usted construye la infraestructura. La infraestructura construye la compañía.

Windows Server System lo ayuda a que usted y su compañía alcancen sus objetivos de manera más rápida y sencilla. Windows Server System le permite:

Comunicarse y Colaborar externa e internamente.
Integrar los procesos y aplicaciones de su empresa.
Analizar la información de su negocio.
Administrar y Operar su infraestructura tecnológica.

En el mundo de hoy, en el que las demandas de IT cambian constantemente, las empresas exitosas son las que pueden construir soluciones de manera más rápida. Hoy más que nunca esas compañías están construidas sobre Windows Server System.





Reduce fast fast!

Microsoft **SQL 2005** Seguridad

Alejandro Ponicke
MCSA-MCSE-MCT
Asesor de Comunidades IT
Microsoft Cono Sur

Reducir la silueta para exponer menos superficie de ataque. Ahí esta el secreto. El DBA se enfrenta comúnmente al reto de asegurar una implementación de bases de datos críticas y sensibles y se encuentra con que el fabricante del motor no lo ayuda demasiado. Muchas decisiones que tomar y pocas certezas al final. Es aquí donde Microsoft hace la diferencia en SQL 2005 al dotar al producto con magnificas herramientas para un control exhaustivo del comportamiento del motor de cara a los desafíos de seguridad del mercado informático actual.

Paseando por un negocio de objetos extraños me encontré hace un tiempo con una KB de Microsoft arrumbada en un estante. Para ser exactos la KB283811, la saque del estante, la desempolvé un poco y con un dejo de nostalgia me pregunte: ¿Porqué esta KB con lo útil que es, con lo importante que es, fue tan poco implementada por los DBAs? Y ahí vino a mi mente la eterna disyuntiva: seguridad o funcionalidad?: Y si después por un problema de permisos la aplicación no anda? Ma' sí! Mejor dejémoslo así, que corra con Enterprise Admin! retumbaba en mi mente como una pesadilla.
Con el lanzamiento de SQL 2005 Microsoft puso de manifiesto una vez más su compromiso en brindar soluciones efectivas y practicas a necesidades cada vez mas importantes como lo es la seguridad en los sistemas informáticos.
La KB del comienzo por si el lector todavía no ha ido a MSN Search : (¿Dónde sino?) a buscarla, explica como configurar la cuenta de servicio de SQL Server para que tenga los permisos y derechos necesarios para correr los servicios de SQL Server sin necesidad de que esta sea administradora del equipo en cuestión ni administradora del dominio. No es necesario explicarle al experimentado lector las consecuencias de tan mala práctica. Ni hablar por cierto de dejar servicios y características ejecutándose "sólo por las dudas".
Ahora que las amenazas de seguridad a sistemas informáticos no son una utopía ni se ven solo en películas de ciencia ficción, el administrador de bases de datos tiene que contar a la mano con un conjunto de herramientas que le permita en forma clara, concisa y concreta reducir lo que se dio en llamar la superficie de ataque. Exponiendo su sistema lo menos posible, y a la vez logrando el nivel de funcionalidad y performance apropiado.

Pase y vea!

Instalación

Ya desde el comienzo no más uno nota cambios, luego de pasar por el proceso de instalación, donde uno puede elegir claramente que componentes de SQL instalar y cuales no, al terminar el proceso y al hacer una revisión de los grupos y los permisos empieza a darse cuenta de algunas novedades.

Revisando los grupos locales observamos una serie de nuevos grupos relacionados con SQL Server, estos grupos fueron creados por el proceso de instalación y sirven para que SQL controle solito, sí, solito los permisos y derechos de las cuentas con las que se ejecutan los servicios y por lo tanto la pertenencia a estos grupos. Lo importante de estos grupos es que los mismos tienen los permisos justos en el sistema de archivos y registry donde SQL 2005 debe operar. Si observa que usuarios pertenecen a esos grupos notará que son los usuarios bajo los contextos de seguridad con los que se ejecutan los servicios.

Además, notara algunos otros detalles, la famosa cuenta "sa" deshabilitada, la habilitación de la misma corre ahora por cuenta y orden del administrador, sin embargo una buena práctica es dejarla como está y crear una cuenta alternativa.

Estas técnicas se en marcan dentro del concepto "secure by default"

```
Símbolo del sistema
Microsoft Windows [Versión 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrador>net user sqlsrv /random /add
La contraseña para sqlsrv es: av$PD$01

Se ha completado el comando correctamente.

C:\Documents and Settings\Administrador>
```

Figura 1.

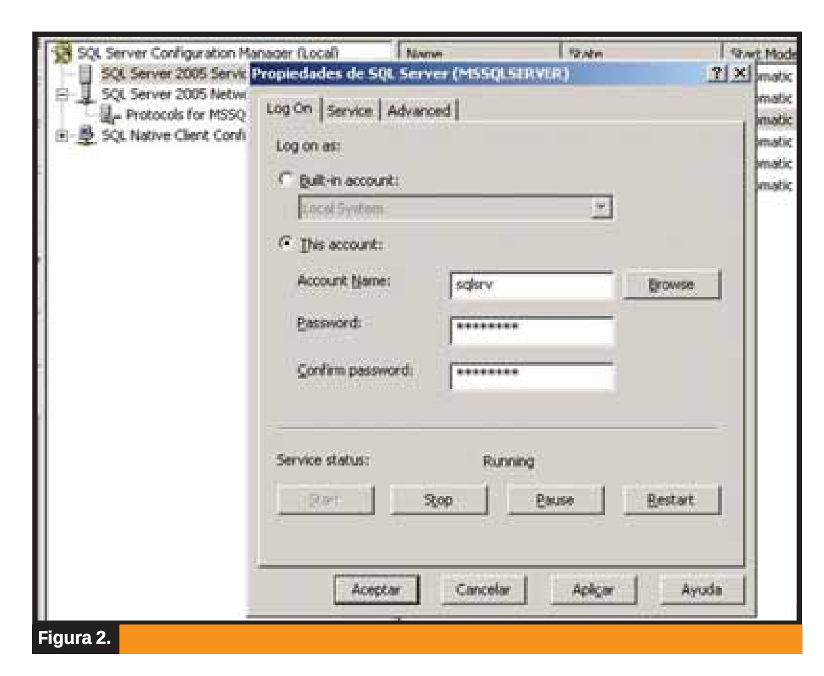


Figura 2.

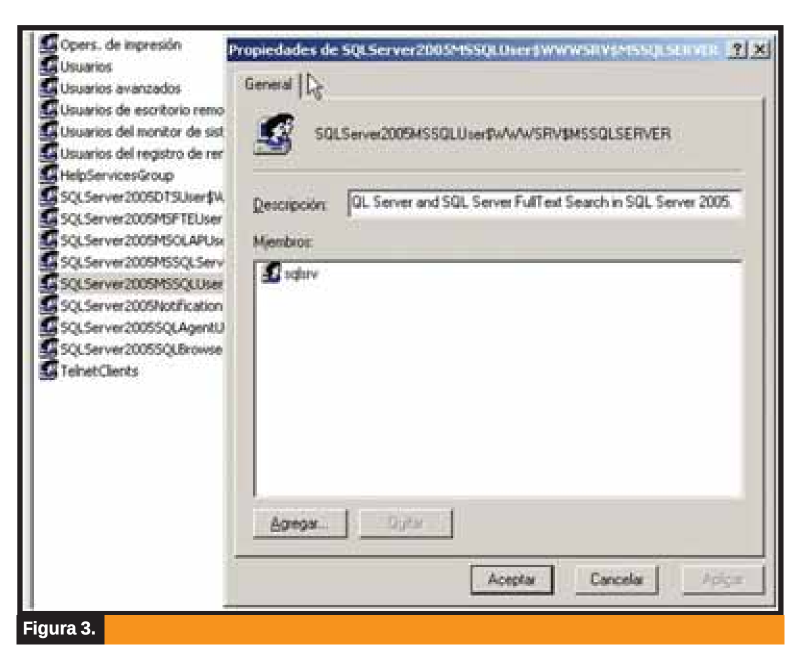


Figura 3.

Microsoft SQL Server Configuration Manager

Esta herramienta debe ser utilizada para configurar entre otras cosas, servicios, protocolos, puertos y alias. Cuando uno utiliza el SQL Server Configuration manager para configurar esas cuentas notará un manejo bastante interesante con relación a las cuentas de servicios.

Veamos un ejemplo

Primero crearemos un usuario estándar al que no se le dará ningún permiso ni privilegio especial (fig.1).

Luego utilizando la nueva herramienta de Microsoft asignaremos ese usuario al inicio de sesión del servicio de SQL Server (fig.2).

Entonces al revisar ahora los grupos locales creados por SQL Server encontramos al usuario *sqlsrv* dentro. Usando la herramienta de administración de usuarios y grupos podemos comprobarlo (fig.3).

Al realizar este procedimiento SQL Server se ocupa por sí mismo de darle los privilegios y permisos necesarios a ésta cuenta sin necesidad de configuraciones adicionales por parte del administrador. Y aún hay más, si uno cambia la cuenta por algún motivo, SQL 2005 sacará de los grupos al viejo usuario y obviamente pondrá al nuevo, haciendo de esta manera un mantenimiento eficiente de sus grupos. Todo el procedimiento descripto anteriormente condenó al olvido a la KB283811 ya que ahora es SQL 2005 quien automáticamente se ocupa de la seguridad de la cuenta de servicio liberando al administrador de tal tarea.

Integración con las políticas de passwords del servidor

En versiones anteriores y de manera predeterminada no era posible asignarle políticas de passwords a las cuentas de usuario de SQL Server con las propias herramientas del motor. Ahora es posible enlazar la política de passwords de SQL Server a la política de password implementada en el servidor ya sea ésta una política local o derivada de Active Directory.

```
USE [master]
GO
CREATE LOGIN [AppUSer] WITH PASSWORD=N'P455w0rd' MUST_CHANGE, DEFAULT_DATABASE=[master], CHECK_EXPIRATION=ON, CHECK_POLICY=ON
GO
```

Los modificadores check_expiration y check_policy del ejemplo superior determinan ese enlace, dotando entonces de un alto nivel de seguridad al subsistema de logines.

Es importante notar que el comportamiento de estas características dependen del sistema operativo donde SQL 2005 está instalado. El óptimo funcionamiento de estas se da con Windows 2003 Server ya que en este caso SQL 2005 utiliza la API NetValidatePasswordPolicy(), no disponible en Windows 2000 Server.

Surface Area Configuration

Al comienzo de la nota hablábamos de reducir la superficie de

ataque, no tener funcionalidades o características habilitadas que no van a ser usadas es parte de la clave del éxito. Es aquí donde se producen muchos de los ataques exitosos ya que al estar habilitadas sin conocimiento del administrador, son explotadas con facilidad ya que son muy proclives a estar poco controladas y mantenidas (fig.4).

Surface Area Configuration es una herramienta que permite cerrar SQL 2005 según las necesidades del administrador. La esencia de esta herramienta es controlar el estado de los servicios de SQL 2005 y todas aquellas características que relacionan SQL 2005 con el espacio exterior. Esta herramienta permite configurar servidores locales y remotos (usando la opción change computer), la única condición es tener los privilegios necesarios tanto en el Sistema Operativo como en el motor de base de datos. No es objeto de esta nota analizar en detalle cada una de las características pero sí repasaremos alguna de las más importantes (fig.5).

Una práctica poco recomendada es acceder a la base mediante el uso OPENROWSET y OPENDATASOURCE sin enlazar los servidores remotos. El administrador tiene entonces la posibilidad de elegir si acepta o no este tipo de conexiones.

Dedicated Administrador Connection es una nueva función que garantiza al menos una conexión al motor usando *sqlcmd* con el modificador *-A*. de esta manera si por algún motivo el motor se comportase de manera errática o se negara a colaborar, el administrador tiene esa conexión garantizada para tomar acciones correctivas.

Además es posible habilitar o deshabilitar las nuevas y viejas funciones de mail, Service broker, HTTP endpoints y demás.

El tan temido *xp_cmdshell*, extended store procedure que permite acceder desde SQL 2005 al sistema operativo y realizar cualquier operación que el usuario impersonado pueda teniendo normalmente privilegios de administrador. La explotación de esta característica ha sido la causante de más de un dolor de cabeza para los administradores.

El tilde en *enabled* marcara la diferencia en cada una de las características arriba enunciadas.

Además del modo gráfico, Surface Area Configuration posee una interfaz de línea de comandos que permite entre otras cosas, importar y exportar las configuraciones para poder aplicarlas de manera más cómoda y eficiente en grandes números de servidores (fig.6).

Luego de recorrer Surface Area Configuration el lector podrá notar que todas las características están desmarcadas, o sea deshabilitadas. Si el administrador no tiene suficiente experiencia podrá verse tentado a habilitar todo luego del proceso de instalación. Pero si se controla la ansiedad, el hecho de habilitar sólo lo necesario, marcara la diferencia entre una implementación segura y responsable de una condenada a las inexorable consecuencias de un ataque exitoso.

Como hemos visto se han hecho grandes mejoras en el control de la seguridad del motor, pero… todo lo descripto en esta nota es sólo una parte de todo lo nuevo que SQL 2005 tiene para ofrecernos en materia de seguridad, aun no hemos hablado de encripción de datos utilizando certificados y PKI, pero eso será en otro momento. ■



Figura 4.



Figura 5.

```
Símbolo del sistema
C:\Archivos de programa\Microsoft SQL Server\90\Shared>sac out sac.conf
Exporting surface area settings for Integration Services instance WWWSRV\MSSQLSE
RVER...Started
Exporting surface area settings for Integration Services instance WWWSRV\MSSQLSE
RVER...Complete
Exporting surface area settings for Full-Text Search service instance WWWSRV\MSS
QLSERVER...Started
Exporting surface area settings for Full-Text Search service instance WWWSRV\MSS
QLSERVER...Complete
Exporting surface area settings for Database Engine instance WWWSRV\MSSQLSERVER.
..Started
Exporting surface area settings for Database Engine instance WWWSRV\MSSQLSERVER.
..Complete
Exporting surface area settings for Analysis Services instance WWWSRV\MSSQLSERVE
R...Started
Exporting surface area settings for Analysis Services instance WWWSRV\MSSQLSERVE
R...Complete
Exporting surface area settings for SQL Browse service instance WWWSRV\MSSQLSERV
ER...Started
Exporting surface area settings for SQL Browse service instance WWWSRV\MSSQLSERV
ER...Complete
Exporting surface area settings for SQL Server Agent instance WWWSRV\MSSQLSERVER
...Started
Exporting surface area settings for SQL Server Agent instance WWWSRV\MSSQLSERVER
...Complete

C:\Archivos de programa\Microsoft SQL Server\90\Shared>
```

Figura 6.

Nota 2

Comenzamos con esta segunda entrega. Los firewalls se han hecho parte de nuestra vida cotidiana. Sirven para algunas cosas, y, a la vez, no sirven para muchas otras. Dicho de otra manera, mucha gente piensa que bastan para asegurar un sistema o una red. Y muchos los utilizan tal cual les llegan de fábrica. Si la configuración por defecto permite realizar las tareas que normalmente se desempeñan, se quedan conformes. Y si resultan demasiado restrictivos, no es raro ver que se los desactive, o se los relaje, hasta el punto de que no sirvan más que para malgastar tiempo de CPU…

En esta segunda nota veremos algunas de las condiciones necesarias y suficientes que nos permitirán plantear un buen esquema de defensa, ya sea de nuestra propia máquina como de toda una red.

Diseñar y mantener un esquema de firewall no es una tarea simple. Pero tampoco es imposible. Requiere una buena dosis de teoría, una buena idea de qué clases de tráfico tenemos en nuestra red, y bastante paciencia.

Como siempre, trataré de obviar ejemplos, para centrarme en las prácticas más recomendables.

Veamos cómo encaramos entonces el desafío. Comenzaremos con el planteo de las medidas de defensa en una máquina, y progresivamente iremos complicando las cosas.

SEGURIDAD en LINUX

Por Luis H. Otegui

De 0 a 100 en 5 notas

Segunda Parte: **Firewalls, Mitos y Verdades**



Ideas básicas

Una buena definición de qué es un firewall la dio en una conferencia el Doctor Steve Bellovin: *"Los Firewalls son barreras entre 'nosotros' y 'ellos', para valores arbitrarios de 'ellos'"*. Entonces, podemos decir que la función principal de un firewall es evitar entradas no deseadas de terceros. OK, como primera aproximación, esta afirmación es correcta. Pero esta idea resulta pobre, o cuando menos, escasa. Un firewall es más que eso; nos permite controlar no sólo el tráfico entrante, sino además aquel que sale, ya sea de nuestra máquina o nuestra red. Y realizar monitoreo y control de todo lo anterior.

Tampoco podemos decir que un firewall sea la solución universal a nuestros problemas de seguridad. Es apenas una parte de la misma. No podemos confiar la seguridad de nuestra máquina, red hogareña o empresa a un firewall. Eso sería negligente. Pero podemos aprovechar sus capacidades para hacer que aquellos que, ya sea por pura curiosidad, o por motivos más oscuros, pretenden ingresar a nuestros dominios, tengan las cosas un poco más difíciles. Así que lo que trataremos de hacer con nuestro(s) firewall(s) es esencialmente lo mismo que con el resto de los otros servicios: permitir sólo aquello que es estrictamente necesario para que las tareas que debemos realizar se puedan llevar a cabo.

Como estamos hablando de Linux, esta nota estará referida a Netfilter, el excelente filtro de paquetes embebido en el kernel desde la versión 2.4, y debido a "Rusty" Russell. Y a su interfaz de comandos, IPTables, nombre con el que mayormente encontraremos referencias en la literatura.

A grandes rasgos, podemos dividir los tipos de firewalls en dos categorías: aquellos que tienen por política por defecto dejar pasar todo, y filtrar algunas cosas, y aquellos que tienen por política por defecto denegar todo, y dejar pasar sólo lo que nosotros queramos. Sobre estos últimos trabajaremos, ya que, a mi criterio, son los más seguros. Plantearlos e implementarlos nos llevará un poco más, pero créanme, vale la pena.

Reconociendo el terreno

Si estamos instalando una máquina por primera vez, lo más probable es que la distro que utilicemos nos haya levantado un firewall mínimo, o que, por lo menos, haya instalado los comandos de espacio de usuario y algunos módulos del kernel. Ahora bien, si esa máquina va a reemplazar a otra que ya teníamos, y de la cual sabíamos bien qué tareas realizaba, o el uso que se le daba, tenemos un buen comienzo. Si en cambio estamos instalando una máquina 100 % nueva, debemos perder un poco de tiempo pensando qué tareas va a desempeñar, qué servicios de red prestará, y cuales estarán desactivados. O puede pasar que a partir de esta nota o de alguna otra se nos ocurra preguntarnos para qué se inicia IPTables cuando el sistema arranca…

Si además tenemos que pensar en exponer servicios al mundo real (un servidor Web, uno de correos, etc.), lo más conveniente será pensar en una DMZ. Las DMZs, o zonas desmilitarizadas por sus siglas en inglés, son redes donde se colocan aquellos sistemas que deben brindar sus servicios al mundo exterior. De esta manera, si un atacante compromete la seguridad de alguno de ellos, no tenga manera de entrar a la red interna de nuestra organización.

Así visto, tenemos dos cuestiones principales: qué hace cada sistema, y dónde lo ponemos. Como norma general, los servidores WWW, de FTP y de correo van a la DMZ, y los de bases de datos, SAMBA, servidores de aplicación y de impresión se quedan en la red interna.

Solo una nota más acerca de la localización de los servicios: está claro que los recursos son limitados, y que no siempre es posible disponer de un equipo para dedicarlo pura y exclusivamente a trabajar como firewall. Pero debemos tratar de no situar en el mismo equipo al firewall de la red y aquellos servicios que ya tienen un largo historial de compromisos, como BIND, el correo, o servidores SAMBA.



Recordemos que si un atacante compromete el firewall, tendrá acceso físico no solo a la red de la DMZ, sino además a nuestra red privada…

En cualquier caso, plantear un firewall a medida (en resumen, todos terminan siendo a medida) implica conocer relativamente bien qué clase de tráfico va a manejar una máquina. Más en el caso de montar un sistema para que se dedique pura y exclusivamente a filtrar tráfico. Pero pongamos esto bien en claro ahora: no por que tengamos un firewall dedicado en la frontera de nuestra red podemos dejar de preocuparnos por montar uno en cada nodo de la misma. Sí, a muchos les parecerá innecesario en sus planteos de red (más a aquellos que vienen del mundo Windows), pero es esencial cuando se habla de una red corporativa. Además de ayudarnos a prevenir accesos no autorizados y derrames de alguna vulnerabilidad en la red, nos ahorrará ancho de banda, y mantendrá la red más limpia.

Una vez que tenemos una idea más o menos aproximada del grado de interacción con sus pares que tendrá una máquina (esto es, servicios a prestar, conexiones entrantes y salientes necesarias, y protocolo de las mismas), podremos pasar a diagramar el firewall para esa máquina.

Mi primer script

Pero volvamos al caso primitivo de nuestra máquina, y su firewall individual. Si no tenemos mucha experiencia con IPTables (de más está decirlo, conviene buscar material, al final de la nota están los recursos), luego de diagramar a grandes rasgos en papel los distintos tipos de conexiones a permitir, lo más conveniente será que volquemos esos datos a un primer script.

Básicamente, las órdenes al kernel acerca de qué hacer con cada paquete se le pasan mediante el comando *iptables*, en forma de una lista de las mismas. Esta estructura condiciona la forma en la que el firewall se comporta: cada vez que llega un paquete, el kernel recorre esta lista de directivas hasta encontrar una que concuerde con una o más características del mismo. Y si no encuentra ninguna, ejecuta la política por defecto. Así que nos conviene poner al principio del script aquellas reglas dedicadas a los servicios que más se utilizan (es decir, en un servidor web, las dedicadas al acceso a los puertos 80 y 443, etc.). De la misma manera, evitemos reglas que repitan una condición, salvo en el caso en que debamos permitir el acceso sólo a determinados hosts. En este caso, tratemos de agruparlas en un solo bloque. Esto nos hará las cosas más fáciles a la hora de mantener el script.

El mismo comenzará por la definición de la política por defecto de nuestro filtro de paquetes. Como hemos dicho, la situaremos en DROP, lo que causará que los paquetes (o *datagramas*, según el protocolo) que alcancen un puerto no definido en las líneas siguientes sea descartado, sin dar ninguna clase de aviso a quien lo envía. Luego, por regla general, si se trata de un firewall para un host que no realiza reenvío de paquetes, sólo trabajaremos con las cadenas INPUT y OUTPUT de la tabla FILTER. En las mismas deberemos especificar una regla de aceptación para cada servicio que queramos que sea accesible desde el exterior. Obviamente, si permitimos una conexión a un cierto puerto y con un cierto protocolo (ya sea especificando la dupla IP de origen/puerto de origen o no), deberemos incorporar el mismo a la cadena INPUT, y asimismo crear una regla correspondiente en la cadena OUTPUT, para que las contestaciones de nuestro sistema puedan salir del mismo.

Una buena práctica es registrar mediante la interfaz a *syslog* que incluye IPTables aquellos comportamientos extraños o inusuales. Y otra, tratar de evitar el *spoofing*, o falsificación de direcciones IP. Para ello, podemos incluir un bloque como el que figura en la Tabla 1 al comienzo de nuestro script.

```
$ iptables -A INPUT -s 255.0.0.0/8 -j LOG --log-prefix "Spoofed source IP"
$ iptables -A INPUT -s 255.0.0.0/8 -j DROP
$ iptables -A INPUT -s 0.0.0.0/8 -j LOG --log-prefix "Spoofed source IP"
$ iptables -A INPUT -s 0.0.0.0/8 -j DROP
$ iptables -A INPUT -s 127.0.0.0/8 -j LOG --log-prefix "Spoofed source IP"
$ iptables -A INPUT -s 127.0.0.0/8 -j DROP
$ iptables -A INPUT -s 192.168.0.0/16 -j LOG --log-prefix "Spoofed source IP"
$ iptables -A INPUT -s 192.168.0.0/16 -j DROP
$ iptables -A INPUT -s 172.16.0.0/12 -j LOG --log-prefix "Spoofed source IP"
$ iptables -A INPUT -s 172.16.0.0/12 -j DROP
$ iptables -A INPUT -s 10.0.0.0/8 -j LOG --log-prefix " Spoofed source IP"
$ iptables -A INPUT -s 10.0.0.0/8 -j DROP
```

Tabla 1: Medidas anti-spoofing en un bastión con dos o más intrfaces

Respecto de a quién se le permite el acceso, siempre que sea posible, deberemos trabajar especificando direcciones IP antes que nombres de host. De esta manera evitaremos la resolución de nombres, un servicio casi trivialmente comprometible. Y haremos el funcionamiento del firewall más rápido.

De más está recordar lo dicho en la nota anterior, deberemos desactivar (y en algunos casos, desinstalar) aquellos servicios no necesarios para el funcionamiento de nuestro sistema. De esta forma, sólo deberemos concentrarnos en defender aquello que necesitemos. Y no deberemos preocuparnos por riesgos asociados a las aplicaciones que corren dichos servicios. De la misma manera, no dejemos puertos abiertos en el firewall porque su uso está planeado para un futuro. Cuanto más económico sea un script, mejor trabajará.

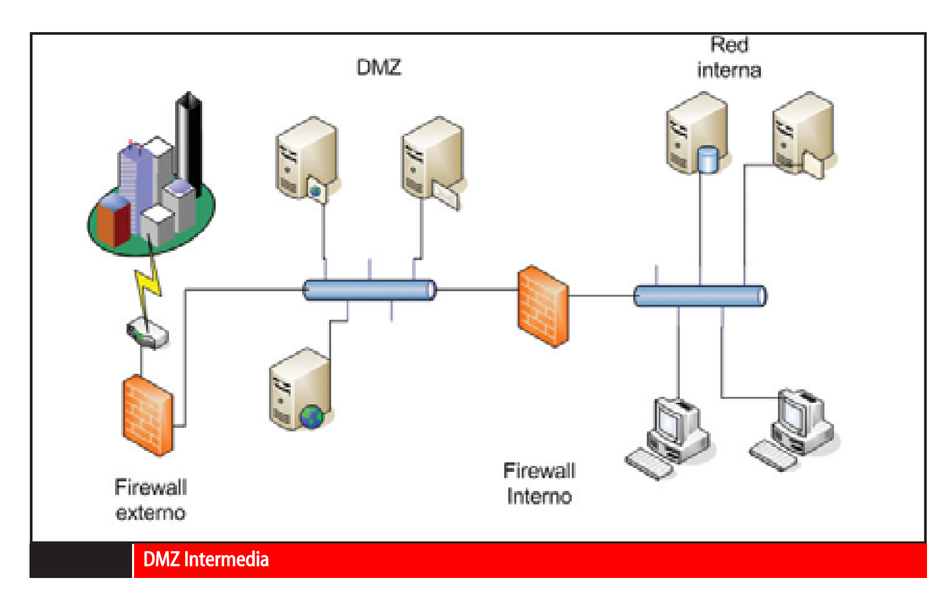
Para realizar la depuración del funcionamiento de nuestro script, podemos echar mano a herramientas como Nmap, Ettercap, o Ethereal. Las mismas nos permitirán monitorear si las conexiones se realizan como deseamos, si nos falta alguna regla para permitir algún acceso, o si alguna es demasiado restrictiva. Lo más probable es que tengamos que agregar alguna regla, o especificar más adecuadamente los hosts a los que queremos permitir acceso. Pero al final, tendremos un script funcional, y que hace lo que queremos, y nada más.

Una vez depurado y probado el script, deberemos incorporarlo al arranque de nuestro sistema. Existen varias maneras de realizar ésto, pero la más conveniente es asegurarnos de que sólo las reglas que nosotros deseamos están activas en el kernel, y guardar este estado mediante el comando *iptables-save*. El mismo nos devolverá a pantalla un listado ordenado de aquellas reglas que están activas en nuestro sistema. Si redireccionamos su salida, obtendremos un archivo que es legible para la mayoría de los scripts de arranque de *iptables* de la mayoría de las distribuciones. Donde deberemos colocar este script dependerá entonces de la distribución que estemos utilizando, pero a modo de ejemplo, las distribuciones basadas en RedHat colocan sus scripts en */etc/sysconfig/iptables*, y aquellas basadas en Debian lo hacen en */var/state/iptables*. En este último caso, es interesante notar que los estados de firewall activado y desactivado se guardan en dos archivos distintos, uno llamado "active", y el otro "inactive".

El paso siguiente: los firewalls entre redes

Si ya tomamos coraje planteando e implementando un firewall para un host, lo siguiente en complejidad es tratar de plantear un firewall que controle el paso de información entre dos o más redes. El caso más simple es el de nuestra red (hogareña, del trabajo, etc.), e Internet. Dicho sistema expuesto suele denominarse en la jerga ***bastión***.

Aquí las cosas se complican de alguna manera, pero también se simplifican: en principio, si no



DMZ Intermedia

colocamos ningún servicio en el firewall, no deberíamos permitir conexiones entrantes ni salientes a este equipo, dedicando todos nuestros esfuerzos a trabajar en la cadena FORWARD de la tabla FILTER, y sobre las cadenas PREROUTING y POSTROUTING de la tabla NAT.

Las cosas cambiarán un poco si hemos decidido establecer una DMZ (aunque no es la forma más recomendable, se puede establecer una DMZ con un solo firewall y tres placas de red, colgándola de una de ellas). En este caso, habrá que considerar si los sistemas que se colocarán en la DMZ tendrán IP privada o pública, y el acceso que se debe tener a los mismos desde la red privada de la organización. Por último, nuestro script no debería permitir el tráfico de servicios (WWW, SMTP, POP, IMAP, FTP, etc.) desde la red interna al mundo, ya que todos los servicios que deseamos brindar se hallan situados en nuestra DMZ.

Como regla general, tratemos de no dejar un acceso vía SSH a nuestro firewall más que desde la red interna. Y si deseamos correr un servidor de nombres en modo caché para las máquinas de nuestra red interna, configurémoslo de manera que sólo acepte peticiones desde esa misma red. Si debemos correr un servidor de nombres para identificar los sistemas expuestos en la DMZ, o lo correremos sobre alguno de ellos, o en última instancia, lo haremos sobre el mismo firewall, pero separándolo del servidor de nombres de la red interna (es decir, con otra instalación independiente).

Ya he comentado que deberíamos colocar los servidores de base de datos en la red interna. La razón de esta medida es evitar que el compromiso de dicho host por ataque directo a algún otro servicio que corra sobre él posibilite la extracción de datos relevantes (ésto es particularmente crítico en el caso de los sitios que manejan *e-commerce*). Es así que deberemos permitir el flujo de datos entre estos servidores y alguna aplicación que corra sobre los servidores web de la DMZ. En estos casos, la comunicación a permitir deberá explicitar sólo las direcciones IP y puertos de los hosts involucrados en la transacción, de manera de ser lo más restrictivos posible. Y, como resulta obvio, deberemos ajustar los firewalls de cada uno de ellos para permitir las conexiones pertinentes.

En el caso de una DMZ, lo que más trabajo nos dará es realizar el emparejamiento de los firewalls de los sistemas expuestos, del bastión que trabaja como firewall principal, y de las aplicaciones en sí. Pero, como dije al principio, si tenemos una buena idea del tráfico que pasa por nuestro firewall, con un poco de organización y método lo resolveremos.

Como en el caso del host aislado, nos quedará sólo transferir nuestro script al arranque del sistema, y testear mediante Nmap o algún otro port scanner el desempeño del mismo, desde la red de la DMZ, la red interna, y el mundo exterior.

Consideraciones de seguridad

Un punto a considerar respecto de la seguridad, y que muchos dejan de lado: en un firewall dedicado, no debería estar instalada ninguna herramienta clásica de *Ethical Hacking*: ni Nmap, ni Ethereal, ni Ettercap, ni Nessus; ni ninguna de las que no nombro. Tampoco en ninguno de los sistemas colocados en la DMZ. En la eventualidad de que queramos analizar el tráfico, o monitorear la actividad en busca de intrusos, nos convendrá enchufar físicamente nuestro propio sistema a la red de la DMZ, o bien utilizar alguna distribución de tipo *LiveCD* al estilo Knoppix STD o ASC en alguna notebook, y luego, desenchufarnos.

La razón es simple: en la eventualidad de que algún sistema de la DMZ o el propio firewall resultaran comprometidos, les estaríamos regalando en bandeja de plata a nuestro atacante aquello que más codicia, y que peleará por instalar en nuestro sistema: un completo set de herramientas. Esto es más crítico aún en el caso de que el sistema vulnerado fuera el bastión, ya que todo el tráfico entre nuestra querida y mimada red interna, la DMZ y el mundo exterior atraviesa este sistema. Es así que volvemos

a la máxima que rige estas notas: cada sistema debe tener instalado sólo aquello estrictamente necesario para que funcione…
Asimismo, nuestro bastión no debería tener más que un usuario real (el nuestro), y no permitir además las conexiones a SSH como root, sino sólo como este usuario, y desde la red interna. Si deseamos instalar un IDS o NIDS en él, del tipo Snort, deberemos tomar todas las precauciones necesarias para asegurarnos de que ninguna información relevante salga por la interfaz pública. Si deseamos compilar algún software que no se encuentra en forma de paquete instalable para nuestra arquitectura y/o distribución, es preferible realizar esta compilación en algún otro sistema, y luego copiar los binarios y librerías resultantes al bastión en cuestión. Herramientas como *make*, *automake* o *gcc* no deberían estar presentes en un cortafuegos, ni en los sistemas de la DMZ.

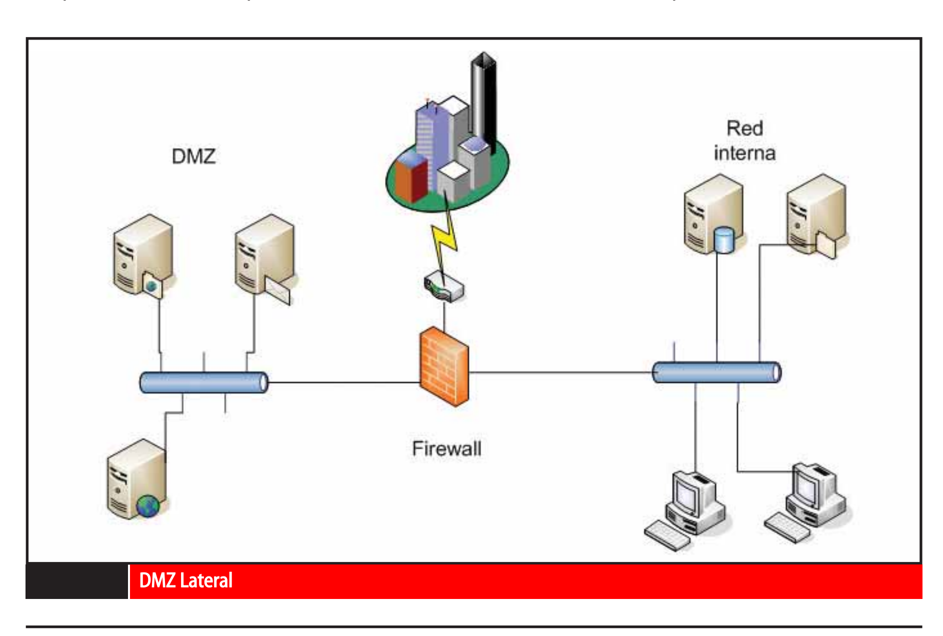
Interacción con otros servicios

Una buena medida (pero que escapa al espíritu de esta nota, y será tratada más en detalle en otra sucesiva) es tratar de implementar proxys a nivel de aplicación cuando sea posible. Ésto es, tratar de encaminar todo el tráfico de algún servicio a través de un Proxy. El más conocido es Squid, en el caso de tráfico HTTP y FTP. Configurando nuestro firewall para obtener un Proxy transparente, lograremos tener un adecuado control del flujo de datos sobre estos dos protocolos.
Ahora bien, es posible que algún usuario trate de realizar túneles desde la red interna a través de un Proxy de aplicación, exportando servicios que nosotros decidimos no permitir. Algunos ejemplos son los programas de tipo *peer 2 peer* (p2p), o los túneles que se intentan para acceder a servicios de mensajería. En estos casos, es posible compilar sobre el sistema bastión algunas extensiones a IPTables, como IPP2P o L7. Ambos proyectos tienen la misma meta: lograr el control y bloqueo eventual del tráfico de tipo p2p. La desventaja es que implican una recompilación del kernel, por lo que en caso de querer instalarlos, habrá que pensar en obrar como se explicó arriba (compilando los módulos y el nuevo kernel en un sistema similar), o bien realizar esta compilación e instalación con nuestro sistema recién instalado, pero luego asegurarnos de borrar toda herramienta de compilación.

También es posible utilizar a IPTables como un sistema de control de ancho de banda, o *shaping*. Las dos extensiones arriba mencionadas se pueden usar, pero existen recetas mucho más simples disponibles en el sitio web del Linux Advanced Routing And Traffic Shaping Howto.

Conclusiones

Como en casi todo lo que tiene que ver con seguridad, la organización y el método a la hora de trabajar son los principales actores a la hora de implementar un esquema de firewalls, ya sea que exportemos servicios o simplemente deseemos navegar por Internet. Y su basamento es el conocimiento. Rusty Russell ha hecho un buen trabajo al plantear el esquema de IPTables y Netfilter. Es por ésto que los animo a seguir leyendo desde aquí en los sitios que se mencionan al final de la nota. Pero, como dije al principio, si bien la idea de un planteo integral de seguridad se apoya necesariamente en los firewalls, no está constituida sólo por ellos. Es por eso que en las notas siguientes veremos más acerca de vulnerabilidades y prácticas metódicas necesarias para que podamos dormir un poco más tranquilos. ■



DMZ Lateral

Para seguir leyendo

-Una buena introducción para novatos:
http://www.pello.info/filez/firewall/iptables.html

-Sitio base de IPTables:
http://www.netfilter.org/

-Extensiones a IPTables:
http://www.ipp2p.org/
http://l7-filter.sourceforge.net/

-Traffic shaping cobre Linux con IPTables:
http://www.tldp.org/HOWTO/Adv-Routing-HOWTO/

Comunicaciones Celulares Móviles **Segunda y Tercera Generación**

Ezequiel Eduardo Pawelko
Licenciado en Sistemas de Seguridad en Telecomunicaciones
Ingeniero en Telecomunicaciones

Detrás de cada teléfono celular móvil hay un mundo más que interesante, que hace del móvil el último eslabón de una cadena y no el primero, por lo cual, a lo largo de este artículo, comentaré los eslabones que hay detrás de cada teléfono, y no del teléfono en sí. La Telefonía Móvil es un campo de aplicación tecnológico extremadamente amplio en donde convergen y divergen las tecnologías que dominan el mundo de las telecomunicaciones. Detrás de cada móvil hay conexión a cientos de miles de millones de usuarios móviles y fijos, además de ser hoy parte de la red de acceso a la Red de Redes, Internet.

Todo comenzó con el primer sistema de Telefonía Móvil que introdujo la AT&T en los Estados Unidos en Junio 1946, en San Luis Missouri. El objetivo del sistema era conectar usuarios móviles, normalmente vehículos, entre sí y con usuarios fijos a través de la Red Telefónica Pública. El sistema operaba a 150 Mhz y utilizaba Modulación en Frecuencia (la misma que se utiliza en las emisoras de radiodifusión sonora) enlazando a los móviles con una gran antena y mucha potencia para cubrir distancias de hasta 80 Km.

El sistema fue tan exitoso, a pesar de su pésima calidad, que, a sólo un año de su creación, se ofreció en más de 25 ciudades de los Estado Unidos, alcanzando a unos 44000 usuarios y con un exceso de demanda de unos 22000 usuarios en lista de espera. Para 1949, la FCC (Comisión Federal de Comunicaciones; organismo que regula a las comunicaciones en Estados Unidos) liberó nuevas frecuencias para que el sistema de Telefonía Móvil pudiera cubrir el exceso de demanda. La FCC dividió a los nuevos canales en dos grupos, y otorgó una mitad a la Bell System (AT&T), y la otra mitad a compañías independientes, como RCC (Radio Common Carriers) con la intención de incentivar la competencia y así evitar monopolios que disminuyan la calidad.

No es sino hasta los '60 que se presentan los grandes avances en este campo, cuando la Bell System creó el concepto de Re-uso de Frecuencias, por el cual las áreas de cobertura de antenas adyacentes no podrían utilizar las mismas frecuencias o canales, con el fin de evitar la interferencia en los primeros sistemas de Telefonía Celular propiamente dichos.

Pero la verdadera revolución no se dio sino hasta principios de los '80, cuando se comienza a utilizar el sistema de telefonía celular AMPS, o Advanced Mobile Phone Service, desarrollado por la Bell. Este sistema de Telefonía Celular Analógica trabajaba en la banda de 800 Mhz y permitía a sus antenas cubrir distancias de hasta 20 Km. de radio. AMPS fue muy exitoso ya que se utilizó en muchos países, aunque para mediados de los '80, coexistía con otros nueve principales sistemas celulares a nivel mundial. La diversidad de sistemas predominaba en el continente Europeo, haciendo que los costos de los móviles y equipos sean altos y la compatibilidad, baja. En base a lo anterior, Europa comenzó a trabajar en el diseño de un sistema único de Telefonía Celular Digital. Por aquel entonces el microprocesador había madurado y la tendencia era hacia los sistemas digitales, los cuales mejoraban notablemente la calidad de la voz.

El trabajo europeo dio como resultado el famoso sistema de Telefonía Móvil Celular GSM, denominado inicialmente Grupo Especial Móvil, y luego llamado Sistema Global de Comunicaciones Móviles debido a su amplia aceptación a nivel mundial.

Del otro lado del océano, Estados Unidos creaba D-AMPS, o AMPS Digital, cuyo propósito era aplicar las ventajas digitales, al tiempo de mantener la compatibilidad hacia atrás con los antiguos teléfonos AMPS. Esta tecnología, con algunas pequeñas adaptaciones, fue utilizada en Japón con el nombre PDC.

D-AMPS no pudo manejar la demanda de comunicaciones celulares en Estados Unidos, la cual creció de medio millón de usuarios móviles en 1989 a trece millones en 1993, por lo que la compañía Qualcomm, Inc. desarrolló el sistema de telefonía celular más innovador jamás creado: CDMA, o Acceso Múltiple por División de Código. Dicho sistema vino a solucionar el problema de capacidad al mejorar notablemente la eficiencia en el uso del Espectro de Radiofrecuencias.

Hoy, CDMA y GSM son contrapartes, pero GSM es la tecnología más aceptada a nivel mundial, estando disponible en más de 210 países, incluido Estados Unidos, lugar de donde proviene CDMA.



Arquitectura de una Red Celular

El objetivo fundamental de una Red de Telefonía Celular es comunicar a los usuarios móviles entre sí y con los usuarios de la Red Telefónica Pública, aunque sus funciones exceden el manejo exclusivo de voz, ya que actualmente se orientan con fuerza al manejo de multimedios, tales como datos, voz y video. La arquitectura básica del sistema es la misma desde que la Bell utilizó el concepto de Re-uso de Frecuencias.

Desde entonces en todo sistema de Telefonía Celular la disposición de las antenas en el área de cobertura sigue, teóricamente, un patrón hexagonal debido a que con éste las antenas se encuentran siempre a la misma distancia de sus antenas adyacentes. El hecho de que las antenas que dan cobertura a celdas vecinas sean equidistantes entre sí hace que no se privilegie la cobertura de ninguna. (fig.1).

Como ya se ha comentado, cada celda dispone de un conjunto de canales que no se repiten en ninguna de las celdas adyacentes, para ser consistente con el Re-uso de Frecuencias y evitar la interferencia. Para ésto se ha determinado que se requiere de un mínimo de cuatro grupos de distintas frecuencias asignadas en el área de servicio para formar un patrón regular (como se observa en la figura). Es común que también se utilicen más grupos de frecuencias distintas de manera que la distancia entre dos celdas que usen el mismo grupo de canales sea mayor a mayor número de grupos, reduciendo aún más los efectos interferentes y mejorando la calidad. El número de grupos se elije como una solución de compromiso entre la calidad y la densidad de clientes, ya que a mayor cantidad de grupos y manteniendo constante el tamaño de las celdas la capacidad del proveedor de servicio disminuye.

Debe aclararse que, en la práctica, las celdas no son siempre hexagonales debido a cuestiones topográficas, de restricciones municipales en la locación de las antenas o para favorecer la propagación de las ondas de radio. Es por ello que se deba optar por otras configuraciones de cobertura que se ajustan a cada lugar.

Además de la forma y disposición de las celdas, se definen componentes básicos que son parte de todo sistema de Telefonía Celular Móvil: los Teléfonos Móviles, la Base Station (o BS) y la MTSO (Mobile Telecommunication Switching Office u Oficina de Conmutación Telefónica Móvil).

La BS se compone de una antena, un transceptor y un Controlador de Comunicaciones, todo situado en el centro de cada celda, para que las ondas de radio se propaguen de forma homogénea. El Controlador de Comunicaciones es el encargado de manejar el enlace con el móvil mientras se encuentre en su celda. La MTSO posee la inteligencia del sistema, ya que es la encargada de realizar la conmutación de las llamadas, posee información de la ubicación de cada Móvil dentro de la celda a la que le presta servicio y del perfil de cada usuario para realizar y/o recibir llamadas. Además, la MTSO posee interfases para conectarse con la Red Telefónica Pública, de modo que puedan comunicarse los usuarios móviles con los fijos, además de utilizar la misma red como medio de transporte para poder conectarse con otras MTSO. Ahora bien, todo este sistema debe permitir que las comunicaciones que realicen sus usuarios móviles

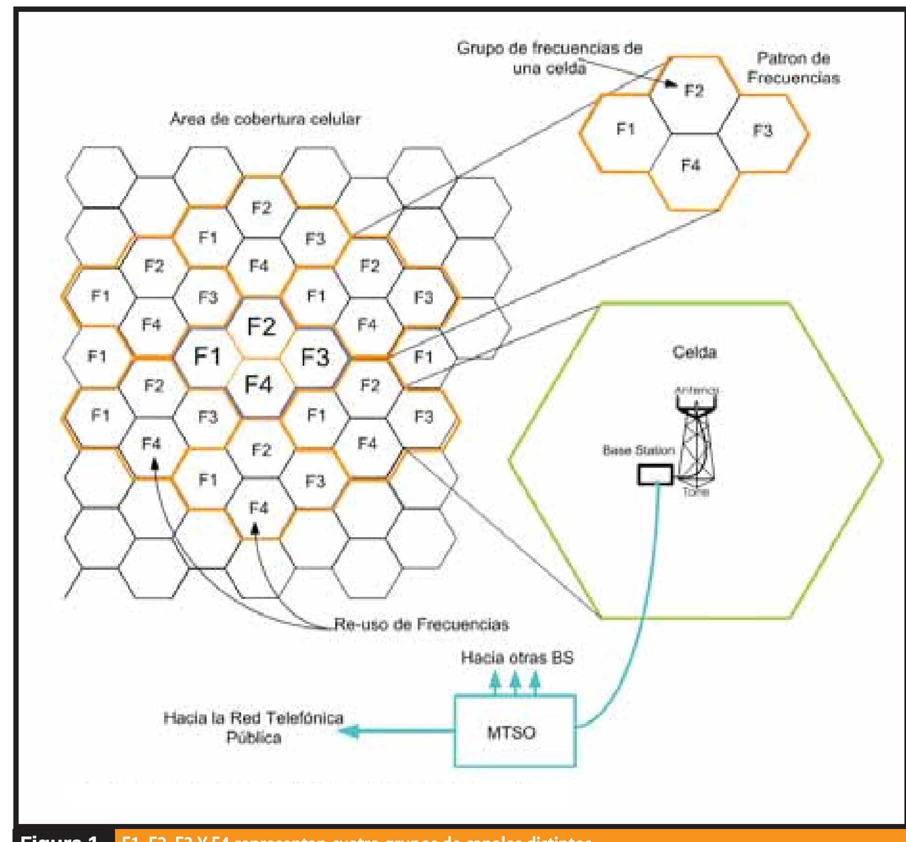


Figura 1. F1, F2, F3 Y F4 representan cuatro grupos de canales distintos

FOTO: © 2004 mobilkom austria AG & Co KG

no se interrumpan cuando el Móvil pasa del área de cobertura de una antena, o Celda, a otra.
En el proceso de pasaje del Móvil de una celda a otra, el sistema realiza un intercambio de frecuencia, o canal, de forma imperceptible para el usuario, todo controlado por la MTSO. Dicho proceso se llama Handoff y es consecuencia del Re-uso de Frecuencia, ya que las celdas adyacentes no utilizan los mismos canales.
El Handoff es una técnica complicada y para su realización debe tomarse ciertos criterios para determinar que el móvil realmente salió del área de cobertura de una base y entró en otra con "mayor señal". En este caso, la MTSO registra en forma continua la posición del móvil y, usando como criterio el nivel de la señal que recibe la BS desde el Móvil, o bien el que recibe el Móvil desde la BS, se compara con el ruido interferente presente en la comunicación y se puede tomar la decisión de cambiar de canal a otro que presente mayor calidad en la comunicación.
En ocasiones el Handoff se presenta debido a la alta interferencia en el canal usado y no porque el móvil esté cambiando a otra celda.
De esta manera, cuando un móvil se enciende busca un canal denominado "canal de control" para comunicarse con la MTSO a través de la BS. La MTSO registra la posición del móvil, la celda en la que se encuentra en ese momento, y verifica el perfil del usuario (para ver el tipo de servicio que puede recibir) y si dicho móvil está o no habilitado. Cuando el Móvil desea hacer una llamada se comunica por dicho canal de control con la MTSO, la cual realiza la conexión con el teléfono destino a través de su propia red, o bien de la Red Telefónica Pública cuando el usuario destino es de telefonía fija, y luego le cede un canal de tráfico. En el caso de que no haya canales de tráfico disponibles la conexión se pierde.
En el proceso anterior, la MTSO se encarga de realizar el establecimiento, mantenimiento y liberación de llamadas que realizan todos los móviles que se encuentren dentro de las celdas a las que presta servicio.
Todo este proceso de comunicaciones y arquitectura es igual en todas las tecnologías, sean analógicas o digitales.

Tipos de Sistemas Celulares Móviles.

Los sistemas de Telefonía Celular Móvil pueden clasificarse en sistemas de Telefonía Celular Móvil Terrestre y sistemas de Telefonía Celular Móvil Satelital. Los primeros son predominantemente de tecnología GSM o CDMA y están formados por los elementos ya vistos. Los segundos, son mucho más complejos y están compuestos por constelaciones de satélites (o grupo de satélites) en donde cada uno de ellos posee diferentes haces que cumplen la función de celdas en su iluminación sobre la superficie terrestre.
Si bien el servicio actual puede ser dado por ambos sistemas, lo que no se discute es qué tecnología utilizar, ya que hoy día los sistemas de Telefonía Móvil son esencialmente digitales debido a las ventajas que presentan dichas técnicas de tratamiento de la información. Las técnicas digitales permiten detectar y corregir errores, proveen seguridad por medio de criptografía, integran diferentes servicios en un mismo sistema de comunicaciones y aumentan la capacidad de transferencia de información utilizando el Espectro Radioeléctrico de una forma más eficiente.

GSM

El Sistema Global de Comunicaciones Móviles, como se lo conoce hoy día, es el sistema de Telefonía Celular Móvil más utilizado en el mundo, con más de 210 países que lo implementan alcanzando el 99% del mercado global. Si bien esta tecnología es la más aceptada, no tiene nada de revolucionario a nivel técnico y su éxito se debe principalmente a su amplia aceptación, que redujo precios y mejoró la interoperabilidad.
Su principio de funcionamiento es similar al del D-AMPS y para su operación utiliza dos técnicas bien conocidas que administran el acceso de los Móviles o BS´s al medio de acceso que es el Espectro Radioeléctrico asignado. Una de las técnicas utilizadas se conoce como Múltiplexación por División de Frecuencia, o FDM, la cual consiste en dividir a la porción de Espectro Radioeléctrico asignado a GSM en segmentos bien definidos denominados Canales de Frecuencias. El conjunto de canales que se obtiene se divide en dos grupos, uno utilizado para la comunicación de Móvil a Base y el otro para la comunicación de Base a Móvil.
Para obtener los Canales de Tráfico, en los cuales los usuarios transmiten la información, GSM finalmente subdivide a cada Canal de Frecuencia en 8 ranuras de tiempo. Esta técnica es conocida con Múltiplexación por División de Tiempo, o TDM, y permite en dicha aplicación que cada usuario acceda a su canal de información en intervalos de tiempo bien definidos. Por tanto, GSM primero divide el Espectro asignado en Canales de Frecuencias (FDM) y luego los divide en ocho intervalos de tiempo (TDM), para ser usado por los Móviles GSM.
Es de destacar que los móviles GSM no tienen la capacidad de trasmitir y recibir al mismo tiempo por cuestiones de costo. Esta simplificación en el diseño es totalmente imperceptible para el oído humano ya que los teléfonos procesan la información a una velocidad muy elevada.

CDMA

El sistema de Telefonía Móvil Celular CDMA, o Acceso Múltiple por División de Código, utiliza una técnica denominada DSSS, o Espectro Extendido por Secuencia Directa, la cual es utilizada ampliamente en todo tipo de enlace de radio que emplee para su trasmisión las bandas de frecuencias que no requieren de licenciamiento, denominadas ISM (Banda de Frecuencia para fines Industriales, Médicos y Experimentales), como IEEE 802.11.
Mientras que en los sistemas clásicos de telecomunicaciones utilizan FDM y/o TDM para lograr el acceso a los canales, DSSS utiliza una idea extremadamente distinta.
Cuando se usa DSSS todos los usuarios utilizan todo el segmento de espectro disponible, por lo





que se conoce como Espectro Disperso o Spread Spectrum.
En esta técnica, cada usuario ve a los demás como interferencia debido a que sus señales colisionan entre sí. Sin embargo, dicha interferencia no evita la comunicación, siendo esta característica parte del principio de operación del Spread Spectrum.
Para lograr su cometido, en CDMA la Base Station asigna un código a cada Móvil para que con él codifiquen la información a transmitir y decodifiquen la información que reciben. El proceso de codificación y/o decodificación se realiza por medio de propiedades matemáticas que permiten extraer la información codificada, usando el mismo código, desde un espectro sumamente interferido por otras comunicaciones.
Esta técnica es difícil de implementar, pero tiene beneficios significativos en comparación con otras técnicas, como las empleadas en GSM.
Principalmente, y como razón de su aparición, mejora notablemente la eficiencia espectral de manera que pueden funcionar más equipos CDMA al compararse con equipos que empleen las técnicas clásicas FDM y/o TDM en un mismo ancho de banda y con las mismas exigencias de calidad. Por lo anterior, la FCC exige, desde hace tiempo, que en las bandas de frecuencia ISM se emplee este tipo de técnica, debido a que se requiere alta eficiencia espectral para que convivan diversos y numerosos sistemas de telecomunicaciones en una misma banda.
Es de destacar que el tema de la eficiencia espectral está en la agenda de todos los organismos nacionales, como la Comisión Nacional de Comunicaciones en nuestro país o la FCC en Estados Unidos, e internacionales como la ITU (Unión Internacional de Telecomunicaciones) que tratan sobre la regulación del Espectro Radioeléctrico. Al respecto, recordemos que en el Espectro convive una serie de ondas radioeléctricas distinguidas por sus frecuencias y pertenecientes a servicios que incluyen, pero no están limitados a TV Analógica, TV Digital, Radiodifusoras de FM, Radiodifusoras de AM, Telefonía Celular, los que demandan más ancho de banda para aumentar su mercado potencial. El Espectro es limitado y ciertas frecuencias son más ventajosas para determinadas aplicaciones que otras, haciendo que su demanda sea grande, por lo que la eficiencia en su uso debe ser un requisito para responder adecuadamente a la demanda del mismo. En Telefonía Celular las frecuencias asignadas son también limitadas, por lo que las técnicas empleadas deben ser eficientes. Tal es el caso de la escasez de frecuencias, que no es posible que muchos proveedores puedan convivir en una misma zona geográfica por las razones comentadas. Desde el momento que se diseña un sistema de este tipo, la ITU recomienda a las entidades reguladoras nacionales que reserven cierto ancho de banda para dichas aplicaciones.
En este contexto, mientras que CDMA apunta a la eficiencia, GSM no lo hace, aunque la siguiente generación de teléfonos a la que estas tecnologías están evolucionando si lo hacen.
La segunda ventaja que tiene CDMA es que posee seguridad sin mecanismos adicionales. El principio de funcionamiento de esta técnica genera privacidad sin la necesidad de incurrir en algoritmos criptográficos. La seguridad reside en el código empleado para realizar la codificación de la información, y, mientras sólo el móvil posea el código, el sistema será seguro.
La tercera ventaja de CDMA tiene que ver con el consumo de potencia debido a que éste es muy bajo, por lo que la autonomía en los Móviles es muy buena. La razón de ésto se debe a que el sistema tiene un control exhaustivo de potencia para que las señales que se reciben en la antena de la Base Station provenientes de cada usuario posean todas las mismas amplitudes. El sistema se encarga de que en todos los casos la potencia sea la mínima necesaria para el correcto funcionamiento de los equipos (fig.2).

Sistemas de Telefonía Móvil Celular Satelital

Los incumbentes en este área de comunicaciones móviles son Globalstar, Iridium e Inmarsat, los cuales poseen constelaciones de satélites generalmente de órbita baja conocidos como LEO (Low

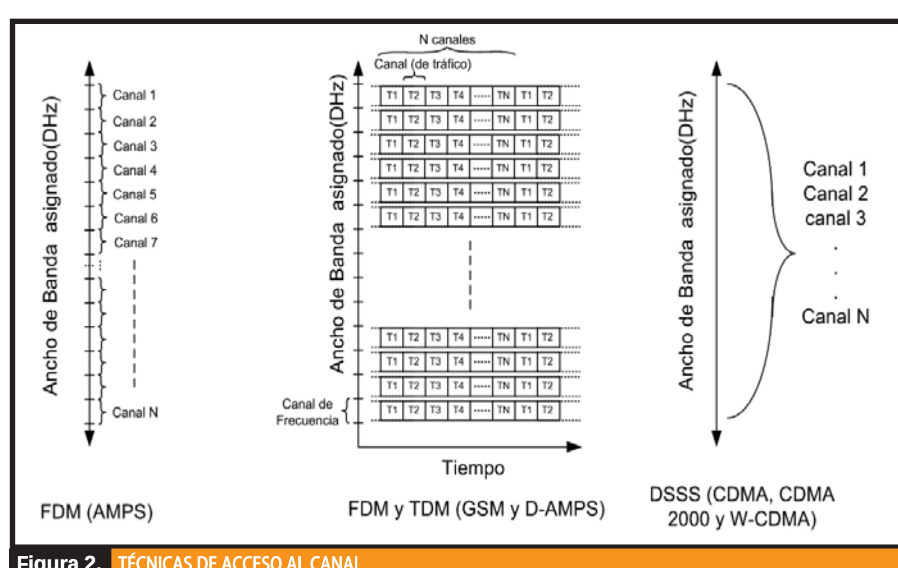


Figura 2. TÉCNICAS DE ACCESO AL CANAL



Earth Orbit). Estos satélites pertenecen a órbitas inclinadas respecto del ecuador con periodos de rotación inferiores a dos horas, por lo que cada constelación requiere de muchos satélites para que siempre haya por lo menos uno visible desde un punto fijo en Tierra.

Cada proveedor de servicio posee un diseño particular en sus sistemas de comunicaciones de manera que las tecnologías empleadas son diferentes, el número de satélites es distinto y la cobertura del servicio a nivel terrestre no es la misma, aunque el objetivo es el mismo: lograr comunicaciones Móviles en lugares que no existe cobertura terrestre debido a que la baja densidad de habitantes no justifica la inversión.

Inmarsat (International Maritine Satellite) es una organización Internacional que provee servicios de comunicaciones móviles marítimas, aéreas y terrestres. Sus servicios son de transmisión de voz y datos y sus teléfonos son generalmente pequeñas valijas que se instalan normalmente en un vehículo. Inmarsat utiliza satélites en órbitas geoestacionarias para alcanzar una cobertura del 98% del globo con sólo cuatro satélites.

Iridium, cuyo nombre proviene del elemento con número atómico 77 debido a que en principio se iban a utilizar esa cantidad de satélites, sólo emplea actualmente 66 satélites (más 7 de reserva) orbitando a 780 Kms. de altura. Es de destacar que es el único sistema satelital que verdaderamente tiene cobertura 100 % global.

Una característica de este sistema es que la conmutación de las llamadas se realiza en el espacio. Cuando un satélite recibe una llamada la dirige a otro satélite hacia su destino, o bien la devuelve a tierra, si el destino pertenece a su huella de cobertura. El diseño de Iridium fue sumamente costoso e impráctico, ya que todos los sistemas electrónicos se encuentran en el espacio y, como se imaginará, es imposible acceder a ellos. Todo ésto hace que el costo de las llamadas sea elevado.

Los teléfonos móviles que se emplean no son mucho más grandes que los teléfonos analógicos de la primera generación o algunos teléfonos grandes de la era digital y se distinguen por poseer una antena que al desplegarla excede en ocasiones el tamaño del propio teléfono.

Globalstar, quien es el proveedor más importante de telefonía celular satelital, emplea una constelación formada por 48 satélites que orbitan de forma inclinada a 1414 Km. de altura, logrando una cobertura de hasta 70º Norte y Sur de latitud, con lo cual su servicio es global, excluyendo los polos.

Este sistema utiliza como técnica de acceso la tecnología CDMA, y la conmutación de las llamadas, a diferencia de Iridium, se realiza en tierra. En Globalstar las llamadas desde un Móvil son levantadas por el satélite que en ese momento esté dándole cobertura, y es inmediatamente redirigida a un Gateway en la Tierra que se conecta con la Red Telefónica Pública para transportar la información hasta otro Gateway, el cual la subirá a otro satélite para entregarla al teléfono Globalstar destinatario. Este sistema es mucho más simple en términos de infraestructura que Iridium, debido a que utiliza infraestructura ya existente, haciendo las llamadas más económicas. A pesar de sus diferencias, los dispositivos Móviles Globalstar son similares a los empleados en Iridium.

Siguiente Generación de Teléfonos Celulares Móviles.

La nueva generación de teléfonos móviles que se avecina es la llamada Tercera Generación o 3G. Mientras que la primera generación de teléfonos celulares estuvo dominada por técnicas analógicas donde el sistema predominante fue AMPS, la segunda generación se conoció como la Era Digital, con dominio de GSM y CDMA. La tercera generación es una nueva generación digital en la que nuevamente dos sistemas se debaten el mercado, siendo CDMA 2000 y W-CDMA los protagonistas. El primer estándar, es la versión 3G del estándar CDMA norteamericano, el cual se diseño para poseer compatibilidad hacia atrás con la antigua tecnología respetando las frecuencias utilizadas por aquel. La segunda norma que representa a la tecnología 3G es la evolución de GSM y se denomina CDMA de Banda Ancha (Wideband). En esta nueva generación ambos competidores han elegido implementar la misma tecnología, ya que sus objetivos son los mismos: Comunicaciones móviles a muy alta velocidad.

Si bien ambos, W-CDMA y CDMA2000, utilizan la misma técnica de acceso, la forma de implementarla es levemente distinta, por lo que no existe compatibilidad entre los sistemas.

Existen numerosas desventajas asociadas al hecho de que presenten múltiples normas, las cuales perjudican a todo el mercado. La incertidumbre asociada de cuál será la tendencia del mercado detiene, en todas las ocasiones, el avance del sector. El hecho de que distintos países o proveedores dispongan de diferentes normas hace que los clientes se vean perjudicados debido a que sus dispositivos móviles no funcionarán en lugares que empleen una norma distinta para la cual fueron construidos.



POR FIN, EL E-MAIL VOLVERÁ A SER UNICAMENTE E-MAIL.

Volvamos a aquellos días en que su e-mail no se confabulaba con virus, gusanos, spam, spam y más spam. Con las soluciones E-mail Security de Symantec, la cantidad de e-mail no deseado que satura las bandejas de entrada de su organización puede ser drásticamente reducida. Con la combinación de más de 20 tecnologías de filtros-spam con el líder en antivirus, las soluciones Symantec E-mail Security erradican el spam, destruyen los virus y bloquean contenidos indeseables y peligrosos. Y con menos desorden en sus e-mails, la gente será más productiva, los tiempos muertos serán menores y al final, su infraestructura se volverá más flexible y resistente. ¿Extraña los e-mails como eran antes? Es tiempo de recuperarlos. Visite www.symantec.com/offer y utilize el código 14132 para obtener mayor información. **BE FEARLESS.**

symantec.™

El por qué de 3G

¿Por qué una nueva generación de teléfonos celulares? Las razones son varias. Primero, el tráfico de datos excede al de voz de la Red Telefónica Pública y su crecimiento es exponencial, a diferencia del segundo que tiende a mantenerse constante. Segundo, se espera que el tráfico de datos exceda al de voz en los teléfonos móviles en poco tiempo. Tercero, el mercado demanda dispositivos móviles que manejen multimedios (datos, voz y video) con mucho ancho de banda de manera que en un sólo dispositivo pueda accederse a todos los servicios imaginables.

Para satisfacer los requerimientos anteriores, los diseñadores de esta generación de teléfonos móviles diseñaron interfaces que trabajan a diferentes tasas de transferencia de información. La primera de ellas es de 144 Kbps y será empleada por usuarios en movimiento a alta velocidad, como en vehículos. La segunda de las tasas es de 384 Kbps y se diseñó para satisfacer a los usuarios que se mueven a baja velocidad, normalmente caminando. La última de las tasas definidas, y que será sumamente interesante para muchos, es de 2,048 Mbps que corresponde a usuarios fijos.

Con las velocidades definidas en 3G, los proveedores podrán diseñar y beneficiarse de un sinfín de servicios, pudiendo los clientes disfrutar de servicios tan esperados como la telepresencia o bien la televisión digital en celulares, además de conexión a Internet de muy alta velocidad.

Para la implementación de esta generación de celulares se ha diseñado lo que se denomina 2.5G, la cual se debe entender como una solución de transición para suavizar la migración desde 2G, hasta que 3G se implemente.

A la 2,5 G pertenece el ya conocido GPRS, o Servicio de Radio de Paquetes Generales, que forma una Red IP sobre el sistema de voz GSM, para proveer comunicaciones de datos a 144Kbps hasta que se realice dicha transición.

Otra tecnología que pertenece a 2.5 G es EDGE, o Tasa de Datos Mejorada para la Evolución de GSM, que no es más que GSM con mayor bitrate o tasa de bits.

Convivencia

Quizás le surjan dudas de qué ocurrirá con otras tecnologías como WiFI o WiMAX en este contexto de altas velocidades. La realidad es que todas convivirán ya que son soluciones que apuntan a distintos nichos de mercado aunque sus implementadores generalmente intenten solucionar todo tipo de problema con una única solución. Ninguna de estas tecnologías es realmente una solución universal que viene a solucionar el problema de conectividad universal. Aquí WiFI soluciona los problemas de Wireless-LAN mejor que cualquier otra tecnología, así como lo hace WiMAX en Wireless-MAN y lo hará globalmente 3G.

De lo que seguramente no hay dudas es que aparecerán dispositivos móviles que puedan funcionar con varias tecnologías inalámbricas, con lo cual los usuarios elegirán la forma de conectarse y de que ninguna tecnología reemplazará a otra.

Conclusión y panorama del mercado argentino

El análisis más interesante en cuanto a la telefonía celular quizás ronde a su fenómeno de crecimiento exponencial en cuanto a la demanda. Cuando hablamos de telefonía celular hablamos de más de 2000 millones de usuarios en todo el globo que la utilizan, y con un crecimiento acelerado que obliga a los proveedores, no sólo a aumentar sus áreas de cobertura, sino también a proveer nuevos servicios que requieren de nueva y más moderna tecnología. Todo ésto ha hecho que la evolución en este campo no se detenga y que surjan avances de forma continua.

En relación al consumo, el mercado argentino asciende a más de 22 millones de usuarios de Teléfonos Móviles, alcanzando casi un 58% de penetración. El crecimiento de usuarios va de unos 140 mil en 1993 a más de 22 millones al día de hoy, y el fenómeno es más destacable cuando se compara con el número de líneas de Telefonía Fija que solo asciende a 8 millones, con un bajo crecimiento. (fig.3).

Como todo lo que se acelera en algún momento tiene que detenerse, el fenómeno seguramente se desacelerará cuando alcance un 66% de penetración (según los estudios de mercado más recientes), lo cual se estima que se dará en este año como consecuencia del límite que representa la línea de pobreza. La desaceleración hará que los prestadores apuesten a estrategias destinadas a posicionarse como vanguardistas, ofreciendo servicios de alto valor agregado como TV móvil y comercio electrónico móvil (M-Commerce), entre otras. También se espera que al saturarse el mercado se mejore la calidad del servicio, que funcionará en parte como discriminante.

A nivel mundial, con la llegada de 3G, la dependencia de este tipo de tecnología será aún mayor a la que conocemos hoy, ya que se ha diseñado para satisfacer la demanda de comunicaciones móviles presente y futura durante mucho tiempo haciendo que se aproxime un periodo en donde reinará, sin dudas, la Convergencia Digital. ■

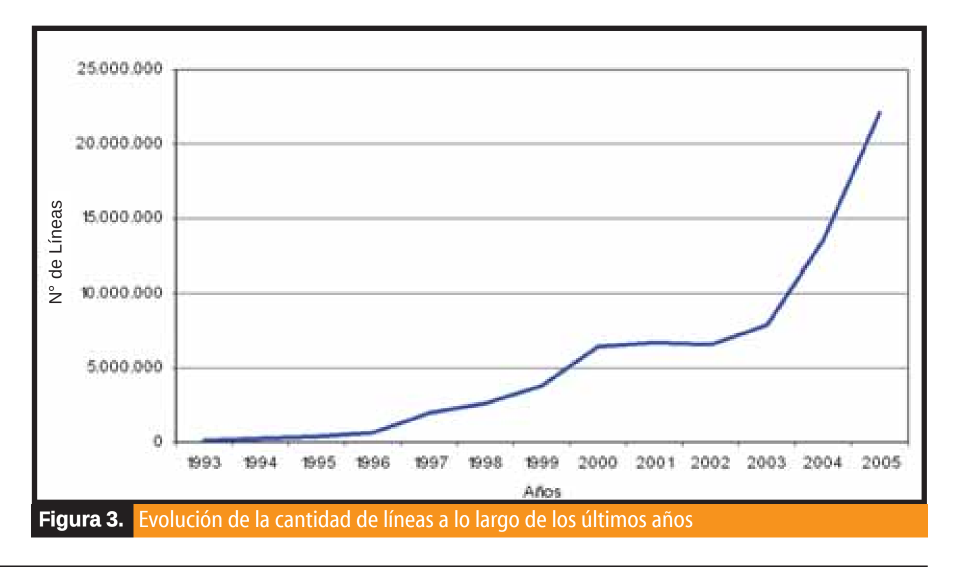


Figura 3. Evolución de la cantidad de líneas a lo largo de los últimos años

U$D100 Laptop Project
¿Existen alternativas?

En un artículo reciente del New York Times (publicado el 30 de enero 2006), John Markoff hizo un análisis de la situación actual del proyecto U$100 laptop (ver: http://laptop.media.mit.edu y Fundación One Laptop Per Child [OLPC]). En el foro de Davos, Bill Gates propuso una alternativa a la idea de Negroponte basada en la idea de celulares. Conozcamos detalles de esta y otras alternativas.

Dr. C. Osvaldo Rodríguez

Para aquellos que no están al tanto, se trata de un proyecto propuesto por Nicholas Negroponte (ver Gente e Historia en IT en esta revista: ¿Quién es Nicholas Negroponte?) fundador del Massachussets Institute of Technology Media Lab (MIT) y director de OLPC. La idea es la creación de una Laptop de U$D100 con conectividad wireless, parlantes estéreo, una manivela para generar electricidad y una pantalla que tendría visibilidad aún bajo luz natural intensa. La ambición de Negroponte de OLPC es poder distribuir dichas máquinas en sociedades carenciadas, dándoles a los niños acceso a los beneficios de la sociedad de la información.

Mucha gente cuestionó la factibilidad de tal proyecto. Negroponte ha afirmado tener el compromiso de 7 países que aportarían U$D700 millones (Tailandia, Egipto, Nigeria, India, China, Brasil y Argentina) quienes comprarían 7 millones de laptops.

No fue hasta el acuerdo con Quanta Computer de Taiwan, (fabricante de 1/3 de las laptops del mundo) que utilizaría inicialmente un chip de AMD, que el proyecto no parecía realizable.

Durante casi un año ha habido interacción entre Microsoft y Negroponte para utilizar una versión de Windows CE que sería preparada para ser expuesta en una versión open-source. Steve Jobs (CEO de Apple) habría ofrecido una versión de OS X.

Finalmente Negroponte decidió por la instalación de un Linux.

"Elegí open source porque es mejor", dijo Negroponte. "Tengo 100 millones de programadores con los que puedo contar".

Uno de los cuestionamientos de especialistas apuntaron al problema de conectividad a Internet de cada laptop que puede costar entre U$24-U$50 por mes en países en desarrollo. La respuesta del proyecto pasa por el concepto de Wireless Mesh Networking (ver NEX IT Specialist #22, pág 64).

Hace pocos días (el 31/1) RedHat y el MIT Media Lab han concretado una serie de acuerdos para colaborar en el proyecto OLPC. Detalles sobre la iniciativa OLPC y el rol de Red-Hat serán conocidos en Junio 2, 2006 al realizarse el Red Hat Summit en Nashville, Tennessee (más info sobre esto en www.redhat.com/promo/summit/).

Pero, ¿Existe alguna otra alternativa a la creación de una laptop de muy bajo costo?

En Microsoft por ejemplo se ha discutido una idea que consideran más barata: transformar un celular especialmente configurado, en una computadora conectándolo a un TV (que sería el monitor) y un teclado.

Bill Gates ha comentado esta idea en CES 2006 (Consumer Electronics Show) de Las Vegas y también la ha refrendado como una alternativa más económica que una laptop en el World Economic Forum de Davos.

La idea de la construcción de una computadora de bajo costo usando un teléfono celular no es ajena al grupo de investigación del MIT Media Group (recordar que Negroponte está en el Board de directores de Motorota INC.) quienes experimentaron la idea de un celular que proyectara un display de computadora sobre una pared junto con la imagen de un teclado que sería operado descifrando el movimiento de los dedos sobre él. Finalmente se decidió por idea de una laptop.

El grupo del MIT trabaja también en el concepto que llaman de "standby bits". La idea es parecida a la manera en que "stanby passengers" (pasajeros standby) consiguen volar con asientos muy económicos en aeropuertos esperando se produzcan lugares a último momento.

El grupo del MIT hará su propuesta al GSM (Global System for Mobile) Consortium (de telefonía celular) de modo de desarrollar un standard que permitiría envío de datos a bajo costo y con propósitos educacionales. Las laptops enviarían y recibirían datos de Internet sólo cuando otros, que pagarían un fee más elevado, no estuviesen transmitiendo.

Muy reciente (Feb 13, 2006)

Nicholas Negroponte ha renunciado como chairman del Media Lab del Massachusetts Institute of Technology para concentrarse en su proyecto de OLPC (One Laptop Per Child). El entrepreneur Frank Moss fue nombrado su reemplazante.



Otra alternativa para llevar computadoras a países pobres es la propuesta por Stuart Gannes, director del Digital Vision Program de la Universidad de Stanford. La idea es simplemente ponerlas en manos de enterpreneurs y hacerlas generar ganancias.

Es claro de las discusiones que cualquiera de los proyectos debería poder tener la ductilidad de poder abordar dos aspectos: el valor educacional y poder fomentar modelos de negocios apropiados.

La pregunta que uno se hace es si el esfuerzo económico de dotar a un niño con una laptop con un neto valor educacional no podría ampliarse al dotar a la familia con una PC económica y acceso a Internet conjugando la componente edicacional y poder ayudar en la salida laboral de la familia. ■

FOTOS: (c) OLPC and Design Continuum

Sistema de Autenticación y Administración de Información Personal

HARDkey MIO



HardkeyMIO es una suite de utilitarios de software asociados a una llave electrónica USB que sirve como elemento físico de autenticación y almacenamiento de passwords.
La misma está compuesta por tres módulos que permiten resolver los principales requerimientos de seguridad.



Disco Privado Virtual

Accede mediante la llave a un área virtual de la PC donde puede almacenar información en forma cifrada.





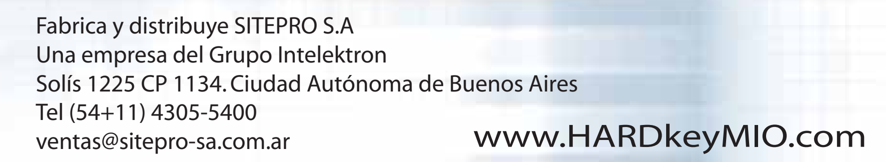
Windows Logon

Reemplaza el ingreso tradicional al sistema operativo mediante usuario y password por una llave electrónica.



Administrador de Passwords

Permite la autentificación automática en web-banking, web e-mail, etc.



Fabrica y distribuye SITEPRO S.A
Una empresa del Grupo Intelektron
Solís 1225 CP 1134. Ciudad Autónoma de Buenos Aires
Tel (54+11) 4305-5400
ventas@sitepro-sa.com.ar

www.HARDkeyMIO.com

SITEPRO
Sistemas y tecnologías de protección informática

Quién es Quién



Steve Jobs

Es una de las figuras líderes de la industria IT, y pionero en la introducción de innovaciones tecnológicas. Junto al grupo de creativos que encabeza, se concentró en productos que se inmiscuyen en nuestros bolsillos mientras musicalizan nuestra rutina, o se lucen sobre nuestros escritorios.

Jobs terminó sus estudios secundarios en 1972 en el colegio Homestead High School, en Cupertino, California, y presenció cátedras dictadas en Hewlett-Packard, en la que consiguió un trabajo de verano. Abandonó sus estudios al cabo del primer semestre de asistir al Reed College en Pórtland, Oregon. Sin embargo su breve paso por la universidad le dejó notables enseñanzas: "Si no hubiera asistido a aquella sola clase de caligrafía en la facultad, las Mac jamás hubieran tenido múltiples tipografías o letras proporcionalmente espaciadas".

Fue Chairman y CEO de Pixar Animation Studios, una productora de films independiente que produjo éxitos de animación como "Los Increibles" y "Toy Story". El 24 de enero de 2006, Disney compró a Pixar, otorgándole a Jobs un asiento en la mesa del directorio, y es ahora el mayor accionista individual de Disney con un 7% del paquete accionario. Creó a Apple Computers Inc. en 1976 a la edad de 21 años, junto con Stephen Wozniak.

En 30 años pasaron de vender la Apple I en el garaje de su casa, por u$d 666.66, a facturar u$d 13.931.000 anuales y a tener 14.800 empleados. Jobs le dio a sus productos lo que siempre escaseó en su vida: simplicidad. Logró un éxito con la inserción de productos electrónicos masivos y de fácil uso para la gente común, acercándoles la tecnología de un modo sofisticado y moderno, quitándole el perfil aparatoso. El exponente máximo de esta propuesta, es actualmente el Ipod.

En 1974, regresó a California (desde Oregon) y comenzó a trabajar como técnico para Atari, una popular compañía de videojuegos.

Ese mismo año, usando lo que ahorró durante los pocos meses en sus nuevo trabajo, Steve viajó a la India, desde la cual regresó con su cabeza rapada y vistiendo ropajes tradicionales hindúes. Tras su regreso, al reintegrarse a su trabajo en Atari, sólo podía ir a trabajar cuando el resto de los diseñadores ya se habían retirado para no molestarlos.

Steve Jobs se casó con Laurene Powell en 1991 y viven en Palo Alto, California, con sus tres hijos en una casa de ladrillos rojos, estilo inglés, construida en los años '30, valuada entre 3 y 5 millones de dólares.

Nicholas Negroponte

Nicholas Negroponte es profesor Wiesner de Media Technology en Massachusetts Institute of Technology, y chairman fundador del MIT Media Lab.

Estudió en el MIT y ha sido un miembro de la facultad desde 1966. Fue el fundador del grupo Architecture Machine Group, un "laboratorio de combinaciones" y un tanque del pensamiento responsable de muchos nuevos enfoques radicales de la interfaz Computadora-Hombre.

En 1982, aceptó la invitación del Gobierno francés, para convertirse en el primer director ejecutivo del **"World Center for Personal Computation and Human Development"**, un proyecto experimental con base en París, diseñado para explorar el potencial de las tecnologías de las computadoras para mejorar la educación primaria en países en desarrollo.

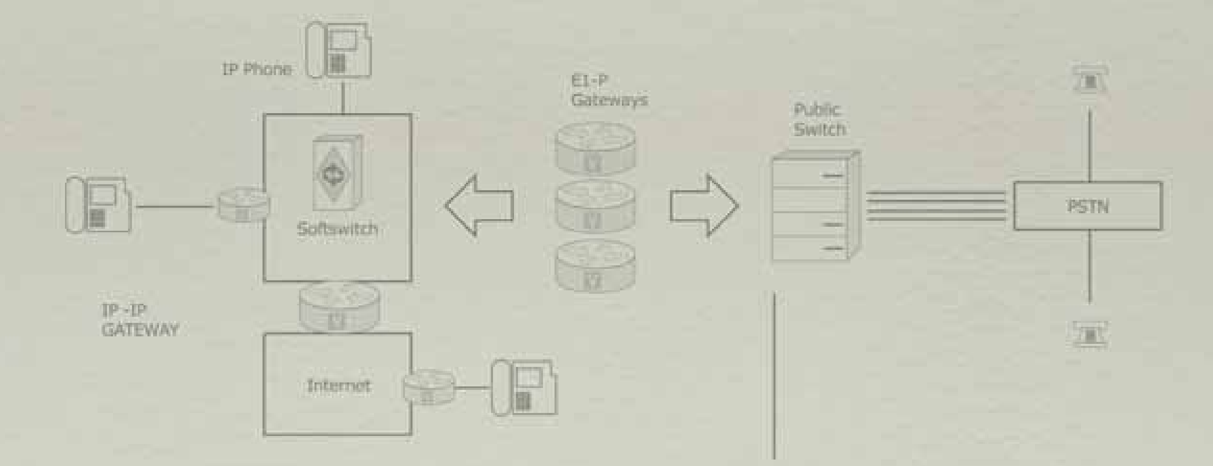
En 1995, publicó *"Being Digital"* que llegó a ser un bestseller del The New York Times, y ha sido traducido a más de 40 idiomas.

En el sector privado, Negroponte trabaja en la junta directiva de Motorota, y como un socio especial general en una firma de capital de riesgo focalizada en tecnologías para entretenimiento e información. Fue fundador de la revista WiReD y ha sido un "inversor angel" apadrinando más de 40 start-ups, incluyendo 3 en china. Ayudó a establecer, y es chairman de la **2B1 Foundation**, una organización dedicada a brindar acceso a chicos en las más remotas y pobres partes del mundo. Negroponte, es chairman de One Laptop per Child (**OLPC**), una organización sin fines de lucros creada por miembros de facultativos del MIT Media Lab para diseñar, manufacturar y distribuir laptops que sean lo suficientemente baratas para proveer a cada niño en el mundo acceso al conocimiento y formas modernas de educación.

"¿Los ricos en información, se volverán más ricos, y los carentes de ésta aún más pobres?"

Con esta frase, ya expresaba en su columna en la Revista **Wired** en el año '98 ("One-Room Rural Schools" de Septiembre) su preocupación por la todavía creciente brecha que separa a los marginados de la informática de aquellos pocos con acceso a la misma.

Link al índice de dichas columnas:
http://web.media.mit.edu/~nicholas/Wired/WIRED6-09.html


IP Phone
E1-P
Gateways
Public
Switch
Softswitch
PSTN
IP -IP
GATEWAY
Internet

¿Cuán **estándares** son los **estándares**?

La mayor parte de las tecnologías se han extendido por el mundo gracias, en su mayor parte, a los estándares, ya sean consensuados o de facto. Mantener y adherir a los estándares es una manera de seguir extendiendo una tecnología, pero además, de mantener las posibilidades de trabajo. Sin embargo, en muchos casos, los estándares no son tan estándares como parecen.



Ricardo D. Goldberger

Periodista Científico

Especialista en Informática y Nuevas Tecnologías. Produce el newsletter electrónico T-knos, conduce *"El Explorador Federal"* por AM Radio El Mundo y colabora en Gillespi Hotel, en FM Rock & Pop.

Muchas de las tecnologías actuales, por no decir la mayoría, se utilizan en prácticamente todo el mundo gracias a la presencia, y su adopción, de estándares de la industria. Tal es el caso de Internet, que gracias a TCP/IP, a http y a HTML, entre otros, ha podido expanderse por todo el mundo.

Un estándar aparece cuando de entre dos o más tecnologías, el uso común, o una organización creada a tal efecto, determina que una de ellas sea la elegida y difundida.

Muchas fueron definidas como estándares por el uso común. Tal es el caso de los archivos doc o xls, que devinieron en modelos por la difusión de las aplicaciones que los utilizaban originalmente.

Esta forma de difusión y adopción, en ocasiones, se debió más a factores de marketing o de publicidad que de calidad de la tecnología. Famoso es el caso del formato de video VHS, que se impuso sobre el beta gracias a la publicidad de sus fabricantes, a pesar de la evidente superioridad tecnológica del segundo sobre el primero. En informática, un caso semejante lo protagonizó el sistema de archivos FAT, que sobrepasó al de Unix ampliamente.

En el caso de los estándares determinados por una organización, en la actualidad no sólo hay muchos que surgieron de esa manera (tal el caso del HTML, XML, 802.11 y todas las variantes y agregados) sino que las propias empresas que participan de un sector del mercado, están prácticamente todas soportando o adheridas a una organización de estándares, ya sea el Web Consortium (W3C), OMA (Open Mobile Alliance) o IEEE (Institute of Electrical and Electronics Engineers).

No son tan estándares

Lo que en realidad hay que tener en cuenta es que un estándar es, en realidad, una tecnología patentada por una compañía determinada. Y las compañías, a pesar de lo que claman, siempre van tratar de recuperar aunque sea algo de lo invertido, ya sea a través de licencias, regalías o el mecanismo que sea más conveniente.

En muchos casos la estrategia de ofrecerlas gratuitamente durante un tiempo les juega en contra, ya que cuando quieren empezar a cobrar por el uso, se encuentran con grandes resistencias. Como ejemplos podemos mencionar cuando Compression Labs quiso demandar a empresas como Adobe, Apple, HP, Xerox y otras más por el uso del JPEG. Algo similar quiso hacer Microsoft el año pasado con FAT. Y no son pocos los que recelan de cualquier compañía cuya tecnología, patentada de acuerdo a los cánones tradicionales, en cualquier momento pase a ser cobrada, como sucede con el formato MP3 y Thomson/Fraunhofer.

El otro aspecto a tener en cuenta son las modificaciones propietarias. Los estándares no son tan estándares como parece, ya que las empresas no resisten la tentación de agregar elementos de sus propias cosechas, con distintos argumentos: porque mejoran la performance, porque aumentan las prestaciones, etc.

El caso más típico es el de HTML. A pesar de ser uno de los estándares más extendidos, por su simplicidad y neutralidad, la forma en que lo interpretan los distintos browsers, así como los tags específicos para cada uno de ellos, hicieron que el HTML sea, en la actualidad, el menos estándar de los estándares. Los desarrolladores y diseñadores de sitios Web saben lo que significa tener que testear los sitios en Internet Explorer, en Firefox, en Opera o en Safari y encontrarse que lo que funciona en uno, queda horrible en otro. Y no hablemos de los intérpretes HTML de los clientes de correo.

Es inevitable que quien diseña, quien desarrolla, quien programa, quiera ofrecerle a sus clientes lo mejor, lo más bonito y lo más rápido. Sin embargo, a veces es mejor "sacrificar" algo de belleza por la funcionalidad de un estándar.

Un estándar, como su nombre lo indica, debe ser capaz de asegurar que la tecnología subyacente funcione de acuerdo a todas las especificaciones y cuando todas las condiciones se cumplen. La difusión de un producto de software, Web o no Web será directamente proporcional a la cantidad de estándares a los que adhiera… o no será.

Validación fuerte por dos factores con **Llaves Electrónicas USB**

Existen pocas empresas Argentinas exitosas, que pueden competir en el mundo del hardware, la electrónica y software a nivel internacional. Los productos "HARDkey" son reconocidos internacionalmente como excelentes. NEX IT Specialist sale en este artículo a conocer las tecnologías detrás de los productos, pero en mayor medida a conocer SITEPRO S.A. Carlos Muller "Gerente Comercial" de SITEPRO SA nos cuenta estos detalles.

Carlos Muller
Gerente Comercial de SITEPRO S.A.

SITEPRO S.A. (www.sitepro-sa.com.ar) es la empresa del **Grupo INTELEKTRON** dedicada a Seguridad Informática y Protección de Software, con más de 14 años de trayectoria en la fabricación y comercialización de sus Llaves Electrónicas. En Argentina más del 85% de las empresas usan nuestras llaves electrónicas para proteger sus desarrollos. Contamos con clientes en casi toda Latino América, España y USA. Además varios de nuestros clientes exportan su software a todo el mundo protegiéndolo con nuestras llaves.

Nuestra principal línea de productos es la compuesta por las llaves electrónicas **HARDkey**, que tienen como principal ventaja que además de su uso tradicional para "Protección de Software y Cifrado de Datos" pueden ser usadas para "Validación de Acceso de Usuarios a Aplicaciones y Sitios Web", ya que estas llaves pueden ser leídas y grabadas en forma remota por medio de Internet y un componente ActiveX que proveemos en el Kit de Desarrollo.

En la actualidad fabricamos varios modelos de llaves, y todas funcionan con el mismo software permitiéndole al desarrollador elegir el modelo que más se adapte a sus necesidades sin tener que modificar sus aplicaciones. Tenemos llaves para puerto paralelo o USB, para uso monousuario o para compartir en una red (controlando el número de licencias concurrentes que se desea habilitar con una sola llave por red), e incluso tenemos llaves con Reloj de Tiempo Real (RTC) ideales para controlar en forma independiente del reloj interno de la PC el vencimiento de esquemas de Alquiler o Leasing de software, o versiones de evaluación con fecha límite de uso.



En los últimos años hemos buscado ampliar nuestro abanico de ofertas, incorporando soluciones que tienden a lograr proteger la información de los sistemas contra accesos no autorizados, por ello hemos desarrollado un producto que denominamos **HARDkey MIO**, que es una llave USB que posee un PIN o clave de acceso, pensado especialmente para ser utilizado como elemento de "Validación Fuerte por Dos Factores": "Algo que tengo" la llave **HARDkey MIO** y "Algo que conozco" su PIN de acceso.

En toda implementación de seguridad existen distintos niveles de requerimientos, y por lo general los usuarios más numerosos son los que necesitan menores requisitos, y sólo para un grupo redu-

Módulos de **HARDkey** MIO Security Suite



Administrador de Passwords

Esta aplicación del tipo SSO (Single Sign-ON) de Windows es un sistema de identidad digital que permite la autenticación automática del usuario al ingresar en Web Banking, Web e-Mail, páginas protegidas con passwords, aplicaciones con login, etc. El almacenamiento de la información sensible se realiza en una llave electrónica de seguridad que se conecta en cualquier puerto USB de la PC. Con la llave y un número de PIN se accede a los datos cifrados, luego el sistema se encarga automáticamente de autenticarlo en sitios y aplicaciones que lo requieran.



Disco Privado Virtual

Este módulo está diseñado para crear un área virtual en el disco rígido de la PC donde se almacena información confidencial en forma completamente cifrada. Al insertar la llave HARDkey en un puerto USB, el sistema permite acceder a esa información como si se tratara de otra unidad de disco dentro del explorador de archivos del Windows. Al retirar la llave, el sistema deshabilita el acceso a los datos totalmente.



Windows Logon

Brinda un nivel adicional de seguridad para su Notebook o PC al reemplazar el ingreso tradicional al sistema operativo mediante un nombre de usuario y password, por una llave electrónica. El acceso a su cuenta de Windows se realiza al insertar la llave HARDkey y tipear un número de PIN. Esto se llama autenticación de dos factores, "algo que tengo" la llave electrónica más "algo que conozco" el PIN.

cido, que realiza las operaciones más críticas, es necesario utilizar mayores niveles de seguridad.
Las llaves electrónicas HARDkey MIO son la solución ideal para lograr una validación fuerte de acceso de usuarios a aplicaciones y sitios Web tal como pide la **Norma ISO 17799**, siendo sin duda la mejor alternativa frente a otros esquemas costosos y complejos de implementar, como
los basados en Certificados Digitales y dispositivos criptográficos.
Normalmente se firman "convenios entre partes" donde se acuerda utilizar cierta tecnología para la identificación de los usuarios, y son suficientes para hacerlos valer entre las partes ya que prevalecen sobre cualquier norma o ley general, con lo cual muchas veces no es imprescindible contar con tecnologías muy avanzadas, sino las más eficientes y económicas.
Las llaves **HARDkey MIO** son la mejor solución costo/beneficio con fácil y rápida implementación y sin costo de "START UP", ni de renovación anual como otras soluciones.
Podemos ofrecer una propuesta "escalable" para obtener una solución única para la "Validación de Accesos de Usuarios" por medio de un método seguro utilizando nuestras llaves **HARDkey MIO**, permitiendo ir implementando en forma escalonada niveles adicionales de seguridad.
En una primera etapa, todo acceso a aplicaciones con USUARIO y PASSWORD puede ser reemplazado o complementado fácilmente con la validación de la presencia una llave **HARDkey MIO**, con sólo agregar unas pocas líneas de código, en las aplicaciones o páginas Web en las que se desea mejorar los niveles de seguridad. Esto es sólo un primer paso, pero resuelve los principales problemas de seguridad para la gran mayoría de los usuarios.
En una segunda etapa se puede incorporar para

Principales aplicaciones de HARDkey

- **Protección de Software y datos**
- **Control de renta o leasing de soft**
- **Cifrado de bases de datos**
- **Control por fecha de vencimiento**
- **Control de aplicaciones en demo**
- **Validación de Acceso a Sitios Web**
- **Almacenamiento de datos críticos**
- **Autenticación de Usuarios con llave**
- **Control de licencias en red**

los usuarios más críticos, el uso de un CSP (Cryptographic Service Provider) que permita con la misma llave **HARDkey MIO**, la cual los usuarios se acostumbraron a utilizar en la etapa anterior, almacenar y transportar Certificados Digitales. Esto sólo implica adquirir la licencia del CSP e incorporarlo al esquema de validación.
De esta forma se puede dividir en etapas el proyecto total, dejando la implementación del esquema de PKI para más adelante permitiendo incluso repartir en el tiempo, la inversión y la carga de trabajo que implican la implementación y puesta en marcha del esquema PKI completo.
Actualmente estamos lanzando al mercado una nueva solución que denominamos **HARDkey MIO Security Suite**, y consiste en un conjunto de aplicaciones que valiéndose de un esquema validación fuerte por medio de nuestras llaves **HARDkey MIO**, permite proteger el acceso a la información almacenada en las PCs contra accesos no autorizados.
La **HARDkey MIO Security Suite** contiene tres módulos principales: un "Control de LOGON a la PC", un "Administrador de Passwords" y un "Disco Privado Virtual Cifrado".
El "Control de LOGON a la PC" permite reemplazar el logón estándar de Windows por la detección de la presencia de la llave **HARDkey MIO** y el ingreso de su PIN, y luego se completa automáticamente el nombre de usuario y password leyéndolos de la memoria de la llave **HARDkey MIO**. Esto permite utilizar "passwords fuertes" (largas y con caracteres raros) ya que no hay que recordarlas ni tipearlas.
El "Administrador de Passwords" es una especie de SSO (Single Sign-ON), que permite el almacenamiento y administración de passwords, de forma tal que no haga falta recordar las passwords de los sitios y aplicaciones de uso habitual, ya que con sólo insertar la llave **HARDkey MIO** y el ingreso de su PIN se completará automáticamente estos datos .
El "Disco Privado Virtual Cifrado" permite mantener segura la información almacenada en el disco rígido de una PC o Notebook. Genera una unidad virtual que se puede mapear como una letra más, y todos los datos almacenados en dicha unidad sólo estarán disponibles cuando se inserte las llave de habilitación **HARDkey MIO** y el ingreso de su PIN. Esta solución permite proteger información confidencial contra robos de equipos o usos no autorizados.
Seguiremos incorporando nuevos desarrollos a la **HARDkey MIO Security Suite** con el concepto de **"todo con una sola llave"**, y accesos seguros por medio de una **"Validación Fuerte de Dos Factores"**: "algo que tengo" la llave **HARDkey MIO** y "algo que conozco" su PIN.

Modelos de llaves **HARDkey**

Llave **HARDkey** RTC USB



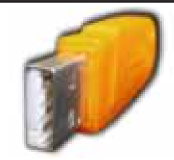
Esta llave posee internamente un reloj de tiempo real (RTC Real Time Clock) que permite controlar fecha de vencimiento de una licencia de uso en forma independiente del reloj de la PC. Con esto el desarrollador logra armar un esquema más seguro ya que el usuario final del sistema no puede alterar el reloj de la llave para extender el uso de una licencia vencida.

Llave **HARDkey** MIO



Mediante esta llave es posible autenticar a los administradores y usuarios de un sistema en forma práctica y segura. La llave de usuario permite aumentar la seguridad introduciendo el concepto de dos factores algo que tengo "la llave", más algo que sé "un número de PIN". Esquemas como estos son indispensables si se pretende obtener certificaciones de seguridad informática como la ISO 17799 para un sistema.

Llave **HARDkey** NET USB



Esta llave puede ser compartida por varios usuarios en una misma red. Posee una memoria no volátil de 4K y opcionalmente, un reloj interno. Permite conectarla y desconectarla con la PC encendida, es ideal para computadoras desprovistas de puerto paralelo.

Llave **HARDkey** STD USB



Su instalación es fácil y rápida. Está diseñada para proteger aplicaciones monousuario. Al igual que el modelo usb de red, posee una memoria no volátil de 4K, lo que la hace adaptable a las necesidades de cada desarrollador. Opcionalmente, cuenta con un reloj para crear esquemas de uso, por fecha de vencimiento.



Llave **HARDkey** NET

Este modelo de protector permite que varios usuarios de una misma red puedan compartirla. También es posible armar esquemas de control de licencias y limitar el máximo número de usuarios concurrentes que podrán utilizar cada módulo del software protegido.



Llave **HARDkey** STD

Basada en un procesador RISC de bajo consumo, esta llave brinda un alto grado de seguridad y transparencia. Ofrece una excelente relación costo-beneficio para protección de aplicaciones mono-usuario y validación de acceso a sitio de Internet. Posee 96 bytes de memoria no-volátil y celdas con funciones especiales.

Zero-knowledge proof
Prueba de conocimiento-cero

Carlos Vaughn O'Connor

En forma abstracta una prueba de conocimiento-cero es una prueba interactiva con un prover y un verifier, donde el prover convence (con alta probabilidad) al verifier qué declaración es verdadera sin revelar ninguna información adicional. Tal prueba es usada en métodos de autenticación. En este artículo brindamos una explicación de qué se entiende por una prueba de conocimiento-cero y dos ejemplos que creemos les aclararán las dudas. Con este artículo NEX IT Specialist ha contribuido a www.wikipedia.org con la versión en español de Prueba de Conocimiento-cero (Zero Knowledge Proof).

El concepto criptográfico de prueba de conocimiento-cero o protocolo de conocimiento-cero es un método interactivo para que un ente pruebe a otro que una declaración (usualmente matemática) es verdadera, sin revelar nada más que la veracidad de la afirmación. Aparece el concepto de "probador" (en inglés "prover") y "verificador" (en inglés "verifier") y se establecen una serie de pasos (protocolo)

Una prueba de conocimiento-cero debe satisfacer las siguientes tres propiedades:

1. Completitud: si la declaración es correcta, el "verificador" honesto (esto es, aquel que sigue el protocolo correctamente) quedará convencido del hecho por un "probador" honesto.
2. Ser lógica: si la declaración es falsa, ningún "probador" deshonesto podrá probar al "verificador" honesto que es verdadera. Excepto, con una probabilidad muy baja.
3. Conocimiento-Cero: si la declaración es verdadera, ningún "verificador" deshonesto aprende algo más que este hecho. Esto se formaliza mostrando que cada "verificador" deshonesto tiene algún "simulador" que, dado el argumento a probar (y ningún acceso al "probador"), puede producir una copia que "parece ser como" una interacción entre el probador "honesto" y el "verificador" deshonesto.

Las dos primeras de estas son propiedades definen el caso más general de "sistemas de pruebas interactiva"

La investigación en pruebas de conocimiento-cero ha estado motivada por sistemas de autenticación donde una parte quiere probar su identidad a la otra a través de alguna información secreta (por ejemplo un password), pero no quiere que el segundo ente conozca nada de cuál es su secreto.

Los pasos típicos en una prueba de conocimiento-cero es que el "probador" da un mensaje de "compromiso" (commitment message) que es seguido por un "desafío" dado por el "verificador" (challenge). Finalmente una respuesta que da el "probador" al desafío. Este protocolo se puede hacer varias veces y dependiendo de las respuestas obtenidas el "verificador" puede aceptar o no la prueba.

Veamos dos ejemplos muy simples pero muy ilustrativos:

Ejemplo 1.

¿"Dónde está Waldo"? es un juego que aparece en libros donde cada página contiene un dibujo muy detallado con muchísimos personajes. El fin del juego es encontrar a Waldo, un personaje predefinido (ver imágen a continuación).

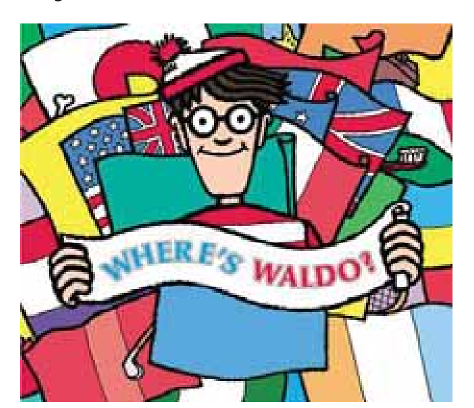
Veamos la siguiente historia que nos ejemplifica este problema de criptografía muy interesante:

Nuestra historia involucra a Alice y Bob (recordar que estos son nombre siempre usados en la mayoría de las ejemplificaciones de temas de criptografía).

Alice y Bob se hallaban jugando a "¿Dónde está Waldo?". Alice de repente exclama: "se donde está Waldo". Bob le responde: "eres una mentirosa". ¿Cómo puede Alice probarle a Bob que identificó a Waldo sin revelar su ubicación en el dibujo?.

Solución simple:

Antes que nada permitamos a Alice tener acceso a una fotocopiadora. Ahora realizan el siguiente protocolo: fotocopian el dibujo específico, Alice corta la imagen de Waldo de la fotocopia (Bob no está autorizado a mirar). Se queda con la imagen de Waldo y destruye el resto. Con esto demuestra a Bob que sabía donde estaba Waldo y revela casi nada nuevo ya que Bob conoce de antemano la imagen de Waldo.



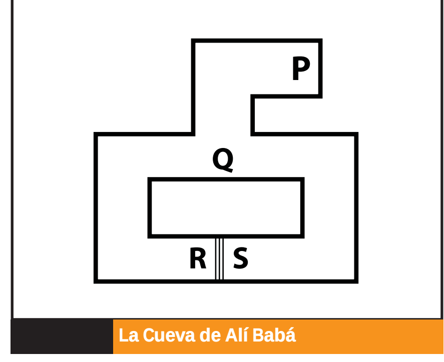
Una discusión más completa puede verse en la web page de Moni Naor, Dept. of Computer Science and Applied Mathematics, Weizmann Institute of Science (Referencia 1).

Ejemplo 2:

La cueva de Alí Babá (no deje de leer las Referencias 2 y 3.).

Alice quiere probarle a Bob que ella conoce las palabras secretas que abren la puerta R-S en la cueva. Pero, no desea revelar el secreto.

El compromiso de Alice es ir a R o S. Una típica rueda del protocolo sería: Bob va a P y espera que Alice vaya a R o S. Bob se dirige a Q y grita a Alice que salga por la derecha o la izquierda. Si Alice no conociese las palabras secretas que abren la puerta R-S habría sólo una chance del 50% de que ella acertara al salir por izquierda o derecha. Si ella realmente conoce el secreto, no importa cuantas veces se repita el proceso siempre saldrá del lado correcto. Y, no reveló la frase "ábrete sésamo". ■



La Cueva de Alí Babá

Referencias

1. *http://www.wisdom.weizmann.ac.il/~naor/PUZZLES/waldo.html*

2. *J.-J. Quisquater , L. Guillou and families, with T. Berson: How to explain zero-knowledge protocols to your children. In G. Brassard, ed., Advances in Cryptology -- Crypto '89, vol. 435 of Lectures Notes in Computer Science, Springer-Verlag, pp. 628-631, 1990.*

3. *FAQ de RSA Laboratorios de RSA Security: http://www.rsasecurity.com/rsalabs/node.asp?id=2152*

TECNOLOGÍA PARA EXPERTOS

SUSCRIPCIÓN $70 ANUALES

- 12 EJEMPLARES NEX IT
EN TU DOMICILIO.

- WEB HOSTING PROFESSIONAL, UN AÑO GRATIS ELSERVER.COM
100 MB DE ESPACIO,
1GB DE TRANSFERENCIA,
5 CUENTAS POP3/IMAP/WEBMAIL,
10 REDIRECCIONAMIENTOS DE MAIL,
1 CUENTA FTP,
ESTADISTICAS DE VISITAS,
EXTENSIONES DE FRONTPAGE 2002,
PANEL DE CONTROL.

- CD ANTIVIRUS PANDA
PLATINUM INTERNET SECURITY 2006
FULL POR 6 MESES

- NEWSLETTER MENSUAL NEX IT
LA INFORMACIÓN MÁS ACTUALIZADA
DEL MUNDO IT

- SEGURIDAD IT
- NETWORKING
- PROGRAMACIÓN
- OPENSOURCE
- SOFTWARE PROPIETARIO
- TENDENCIAS IT
- HARDWARE

suscripciones@nexweb.com.ar
+54 (11) 5031-2287
NEXWEB.COM.AR







ENVIANDO POR FAX O POR CORREO ESTE CUPON OBTENGA DOS EJEMPLARES NEX IT FREE A SU ELECCION

DATOS DEL SUSCRIPTOR

APELLIDO ____ NOMBRES ____
EMPRESA ____ CARGO ____
FECHA DE NACIMIENTO ____ TIPO DE DOCUMENTO ____ N° ____
TEL. PARTICULAR ____ TEL. LABORAL ____ FAX ____
E-MAIL PERSONAL ____ E-MAIL EMPRESA ____
DOMICILIO DE ENTREGA ____ N° ____ PISO ____ DPTO. ____
LOCALIDAD ____ PROVINCIA ____ CÓDIGO POSTAL ____

FORMA DE PAGO

NOMBRE/RAZÓN SOCIAL ____ CATEGORÍA IVA (ADJUNTAR FORMULARIO) ____
CUIT N° ____
EFECTIVO ____ CHEQUE (A LA ORDEN DE EDITORIAL POULBERT S.R.L.) ____ BANCO ____ NÚMERO ____
TARJETA DE CRÉDITO (1 PAGO) ____ VISA ____ MASTERCARD ____ AMÉRICAN EXPRESS ____
NÚMERO ____ CÓDIGO DE SEGURIDAD ____ VENCIMIENTO ____

Editorial Poulbert S.R.L. - Revista NEX IT Specialist
AV. CORRIENTES 531, 1° PISO (C1043AAF), CAPITAL FEDERAL
TEL./FAX.: (011) 5031-2287 - suscripciones@nexweb.com.ar
WWW.NEXWEB.COM.AR

FIRMA ____ ACLARACIÓN ____

Promoción válida solamente para la República Argentina; hasta el 31 de Marzo de 2006 o agotar stock de 150 unidades

Academia Latinoamericana de **Seguridad Informática**



Fredi David Vivas

Líder de Estrategias de Comunicación de Microsoft IT PRO Argentina
www.itpros-argentina.com.ar

La Academia Latinoamericana de Seguridad Informática (ALSI) es sin dudas el proyecto tecnológico-educativo más importante y prestigioso de Latinoamérica.

Dicho así, puede sonar exagerado, pero es claro al revisar algunos números, a saber:

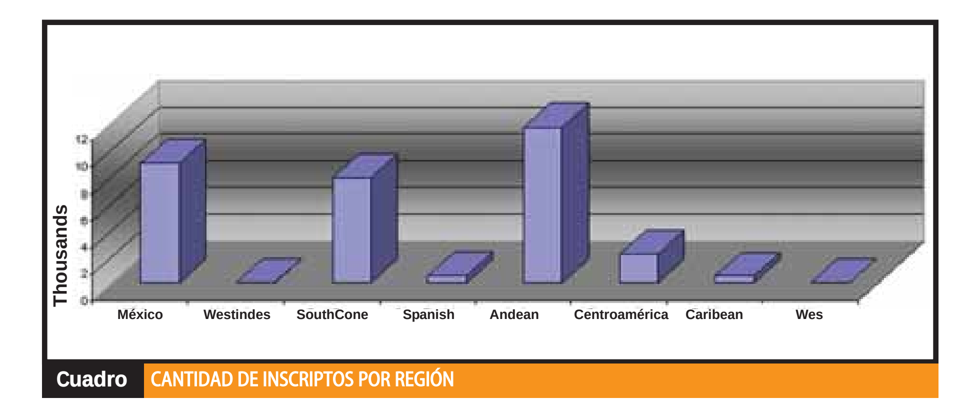
-Desde sus inicios (marzo de 2005) la academia albergó unos 35.000 alumnos de habla hispana.

-El sitio de ALSI recibió 1.379.840 visitas desde enero de 2005.

-Realizo alrededor de 50 Webcast y más de 70 Chats.

-Y lo más importante, todo ésto con costo 0 (si… cero!)

Esta academia on-line esta respaldada por la excelencia académica del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), de E-Modulo Security (Empresa Brasilera de Seguridad) y de ISEC Argentina (Information Security Inc.). Todo ésto coordinado y soportado



Cuadro CANTIDAD DE INSCRIPTOS POR REGIÓN

por el equipo de Microsoft TechNet Latam.
El programa está construido en tres etapas que van aumentando gradualmente su nivel de complejidad. Cuenta con períodos fijos de inicio y fin de cursos, así como fechas de evaluaciones a través de exámenes en línea. Los participantes requerirán un mínimo de 80 % de respuestas correctas en las pruebas online para acreditar los módulos de cada etapa. Sin dudas esta estructura le da un nivel académico interesante y obliga a los alumnos a no dejar pasar el tiempo para darle continuidad a sus estudios.
Los cursos cuentan con sistemas de ayuda en línea como Chats y Webcasts para que los participantes puedan tener acceso a las herramientas necesarias para culminar con éxito el programa. Newsgroups, Weblogs y correo electrónico sirven también para volcar inquietudes y sacarse dudas del material teórico abordado.
Los requisitos para participar en el programa son únicamente contar con conocimientos técnicos en seguridad y lo más importante, disponibilidad de tiempo para poder cursarlo. También necesitarán una computadora con elementos multimedia y conexión a Internet; ésto es indispensable porque todos los materiales serán suministrados y colocados en el sitio Web de Microsoft TechNet Latam, para ser descargados por cada estudiante en su máquina.
Para participar sólo se requiere reservar un espacio dentro del programa, ingresando los datos en la página de PRE-REGISTRO: http://www.mslatam.com/latam/technet/comunidad_ti/Html-ES/frontend/users/default.asp?origen=cso
La información ingresada en este registro permitirá a Microsoft llevar un control y seguimiento del progreso académico de cada estudiante dentro de la Academia. También para servirles de soporte con recordatorios y avisos sobre nuevos materiales, fechas de cambio de módulo, de etapa y por supuesto fechas de evaluaciones y resultados. Este apoyo es importante ya que por la estructura del programa (enseñanza-aprendizaje) es indispensable que todo el proceso en cada módulo tenga principio y fin.
Dicho ésto, recorramos los ejes temáticos, sus objetivos y la forma elegida para alcanzarlos.
La Academia Latinoamericana de Seguridad Informática, como programa educativo, fue diseñada con el objetivo principal de crear una educación formal alrededor de la Seguridad, como tema, transmitiendo el conocimiento sobre los diferentes aspectos que la involucran, basado en sus pilares: Personas, Procesos y Tecnología.
Los 8 módulos de ALSI que conforman las Etapas I y II, acompañan casi de forma lineal a los módulos que conforman la ISO 17799.
En la Etapa I, el objetivo apunta a los profesionales que tienen relación con infraestructura y no tanto con conceptos de seguridad, por ende se focalizó fundamentalmente en separar los conceptos de Seguridad de la Información y Seguridad Informática. Observando que muchos profesionales no pueden pensar en Seguridad de la Información mas allá de un Firewall, IDS, IPS o cualquier otro mecanismo de seguridad de datos.
La etapa I desarrolla los conceptos de Sistema de Seguridad de la información y devela riesgos más allá de los informáticos (virus, accesos no deseados, etc.). Se definen también los conceptos de Activos de la empresa, Amenazas, Puntos débiles, Riesgos aceptados, Ciclos de seguridad y Métricas. En síntesis, se trata de entender que no solamente un Hacker puede dañar la información de una empresa, sino que también es peligroso estar expuesto a un foco de incendio o a un desastre natural, haciendo hincapié en que la información trasciende lo que pasa dentro del cable UTP y demostrando la importancia de lo que está en papel, medios no magnéticos, contratos, etc.
Se forma a los alumnos en los principios de la Confidencialidad de la información y sus diferentes estadíos, también en la interpretación de los tipos de Amenazas y Riesgos.
En el módulo 2 de la etapa I es muy valioso el aporte acerca del Análisis de riesgos, enseñando a confeccionarlo, interpretarlo y poder presentarlo a la Dirección de la empresa.
El tema central del modulo 3 son las Políticas de seguridad, en función del Análisis de riesgos obtenido, con mucha información respecto a diferentes Modelos de políticas.
El modulo 4 es la implementación de estas Políticas y los Planes de seguridad.
Luego de este paneo general, en la Etapa II se trabaja sobre la confección de un SGSI (Sistema de Gestión de Seguridad de la Información), se destaca como éste va necesitando que la empresa se comprometa en su totalidad con el programa de seguridad de la información.
Modulo a modulo se va observando el necesario compromiso de la gerencia para la puesta en marcha del plan y como a ella se suman las áreas Legales, Recursos humanos y otras de importancia.
Se recorre el desarrollo de una metodología de trabajo acorde a los objetivos trazados en el SGSI, en cuanto a Protección de software, Nuevo código, Medidas de seguridad física, Evaluación de riesgos, Planes de continuidad del negocio, Riesgos asumidos y excepciones, diferentes tecnologías de BPC (Business Plan Continuity) y Modelos de implementación de estas tecnologías, por ejemplo MOF (Microsoft Operations Framework).
Recorrimos así las dos primeras Etapas de la Academia, divididas en 4 módulos cada una.
ALSI continua con una última Etapa, pero a diferencia de las otras, ésta será presencial y sus alumnos podrán entrenarse para presentar los exámenes de certificaciones especializadas en seguridad como CISSP (Certified Information Systems Security Professional) y CISM (Certified Information Security Manager).
Cerca de 800 egresados de las Etapas I y II podrán acceder a cursos que se dictarán en las oficinas Microsoft de cada país.

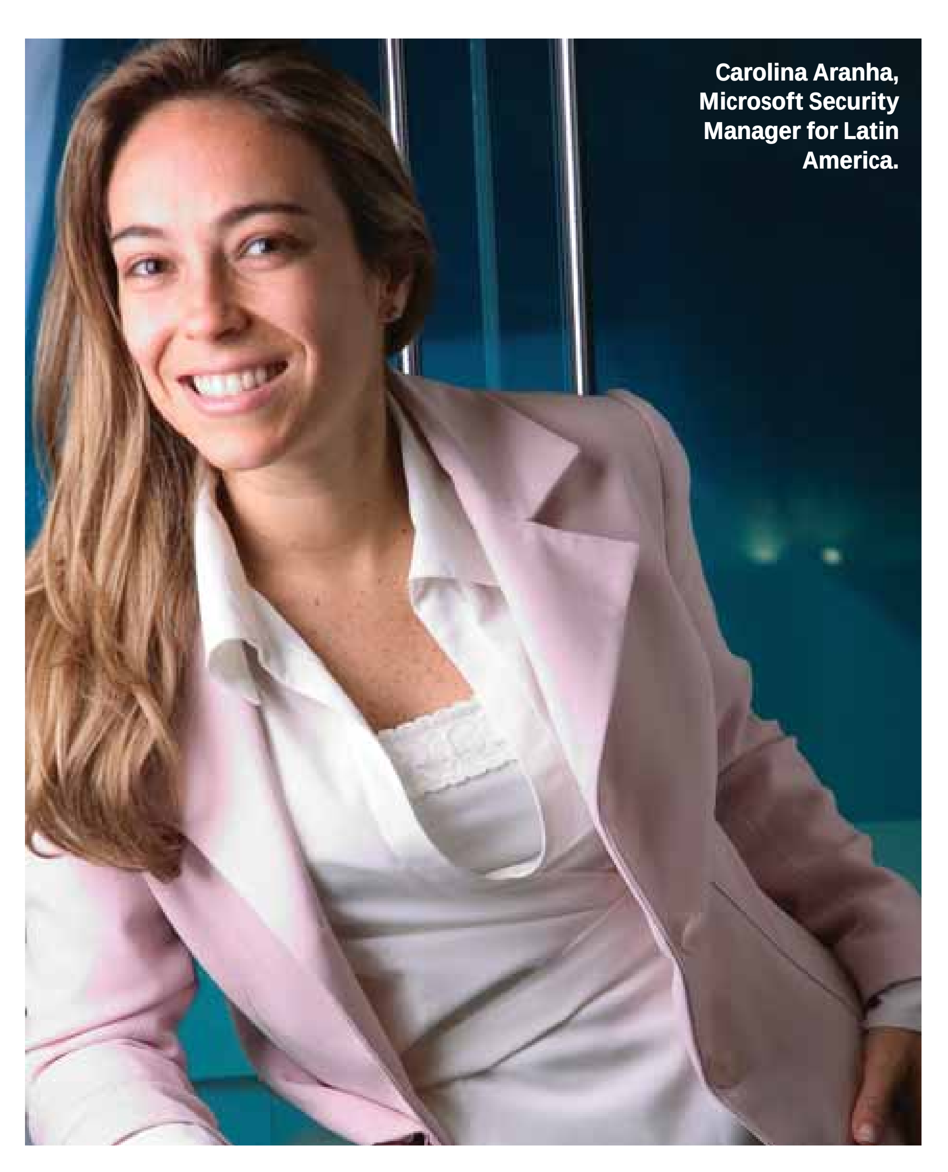


Encuesta Global de Seguridad Informática

Ernst & Young realizó un relevamiento para cuantificar el nivel de seguridad de la información en distintas corporaciones mundiales. En la 7ma. Edición de la Encuesta Global sobre Seguridad de la Información de Ernst & Young participaron 1.235 compañías de distintas industrias que representan algunas de las empresas líderes en 51 países, incluyendo Argentina.

El 80% de los encuestados coincidieron en que la Seguridad Informática no se encuentra entre de las prioridades del CEO.
Mencionaron "La falta de conciencia de los usuarios respecto de la seguridad" como el principal obstáculo para garantizar una efectiva seguridad de la información.
La mayoría de los encuestados identificó como su principal amenaza los virus, Worms o trojan horse y en segundo lugar la inadecuada utilización de los Sistemas de Información por los empleados.
El 77% de los encuestados respondió que tiene un plan de respuesta ante incidentes.

Más Información:
http://www.ey.com/global/content.nsf/Argentina/Home



Conozcamos a Carolina Aranha, Microsoft Security Manager for Latin America, quien nos comentará con más detalle los orígenes y el futuro de este ambicioso proyecto.

¿Cómo surge la idea de armar esta academia de seguridad?
La idea acerca de incrementar el conocimiento en seguridad informática, surge básicamente de recopilar información en la comunidad Microsoft, profesionales en informática, asociados y clientes. Específicamente de las empresas que necesitan profesionales con el adecuado nivel de conocimiento en seguridad.
Al mismo tiempo, la investigación en el mercado de capacitación en seguridad mostró que los cursos con cierta complejidad suelen ser muy caros y los baratos, extremadamente básicos.
Sabemos que como empresa líder del mercado tenemos que ayudar a proveer un entrenamiento consistente que permita a los IT Pros, socios y clientes proteger sus ambientes de una manera efectiva.

Teniendo en cuenta la variedad temática en relación a la seguridad informática ¿Qué parámetros se estudiaron para determinar los contenidos?
Aprendimos que necesitaríamos primero desarrollar distintos niveles para alinear el conocimiento básico en seguridad y segundo, proveer una mirada sobre las claves en temas de mercado, tales como norma ISO 17799 y también preparar a los estudiantes que califiquen en los más reconocidos certificados de seguridad como CISM y CISSP. No necesitamos focalizarnos en tecnología pero si en la gente y los procesos, que son los dos principales pilares en la seguridad informática.
Al mismo tiempo decidimos realizar un entrenamiento al alcance de todos, ésto es un antecedente, con este sistema on-line pudimos tener llegada a más gente del exterior y tener mayores lugares protegidos.

¿Crees que el profesional de tecnología tiene una capacitación insuficiente en relación a la demanda laboral y a la necesidad real de las empresas?
Entendemos que la seguridad informática es algo bastante nuevo y demanda una constante actualización, debido a que existe una rápida y constante evolución. "Por cada muro distinto que construyes hay alguien tratando de encontrar una manera creativa de atravesarlo". Ésto explica porque tenemos constantemente nuevas regulaciones, certificaciones y especificaciones en seguridad. Ésto es por lo que creemos que la constante actualización de conocimientos es siempre imprescindible para los profesionales en seguridad.

Según algunos estudios de consultoras especializadas, las empresas tienen muy baja conciencia de los riesgos de no poseer una política eficiente en relación a la seguridad informática. ¿Qué puede hacer un IT Pro para revertir esta situación?
Muchas empresas creen que protegiendo sus equipos con herramientas como Antivirus y Firewall podrán asegurar la información.
Pero seguridad es mucho más que eso. Tiene que ver con tecnología, personas y procesos. Recomiendo a los IT Pros que asesoren a las compañías en los temas de seguridad que suelen ser problemáticos, demostrando cuáles son los puntos fundamentales a considerar.
Es importante resaltar los riesgos / costos de la falta de una política correcta en seguridad informática.

Pasaron varias etapas I y II de la Academia y en algunos países ya arranco la Etapa III presencial. ¿Cómo se están preparando en el resto de los países y que expectativas tienen?
Ya hemos comenzado en Brasil y capacitado a casi 400 estudiantes en la Etapa III. La respuesta ha sido extraordinaria y el nivel de estudiantes muy alto. Estamos muy entusiasmados en continuar en otros países latinoamericanos. Hemos rastreado los Chat de grupos estudiantiles y vimos que estaban tan satisfechos con la Etapa III que ya se la estaban recomendando a estudiantes de fases anteriores.

¿Qué avances y proyectos tiene planificado Microsoft para la comunidad latinoamericana durante este 2006?
Queremos incrementar el éxito de la Academia, estamos planeando invertir en mejorar el contenido, colocando especialistas que escriban artículos específicos y comentarios sobre temas claves, para proveérselos a los estudiantes a fin de especializarlos en distintos temas de seguridad, tales como desarrollo de seguridad. También participando en grupos que capaciten para certificaciones internacionales. Tenemos además algunas "sorpresas" para el futuro, que estoy seguro harán muy feliz a los estudiantes.

Go!
Ingresa a la Academia
http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp

Home de Microsoft TechNet Latam
http://www.microsoft.com/latam/technet

Conozca cómo es **un examen**.

Certificación CISSP

1. Metodología y sistemas de control de acceso
Dentro de la metodología IDS, el término "firma" ("signature") se define como _____
A. Una llave que está attacheada/adjunta a un mensaje en la forma de un certificado digital.
B. Un patrón de eventos de un ataque basado en intrusiones pasadas.
C. Un patrón de ataque que se repite una vez introducido en un ambiente.
D. Una porción de información que está encriptada para autenticar a un cliente o proceso.

Respuesta: *C*
Las "firmas o signatures" son comúnmente distribuidas por vendors de sistemas de detección de intrusos (IDS) como parte del soporte que dan a un componente de software IDS. Basado en esas firmas los IDS se activan.

2. Seguridad de aplicaciones y desarrollo de sistemas.
Cuando diseño una base de datos ¿Cuál es MENOS importante?
A. Conocer la cantidad de datos.
B. Conocer la importancia de los datos.
C. Conocer la plataforma de hardware.
D. Conocer los requerimientos de acceso a usuarios.

Respuesta: *C*

3. Business Continuity Planning (BCP) y Disaster Recovery Planning (DRP)
BCP apunta fundamentalmente a:
A. Disponibilidad (availability).
B. Integridad.
C. Confidencialidad.
D. Responsabilidad (accountability).

Respuesta: *A*
BCP se refiere básicamente a la Disponibilidad (Availability) de la tríada que define a la seguridad (CID).



Muchos de Uds. habrán escuchado de la certificación CISSP de seguridad informática. Conceptos como que "es la más prestigiosa", "abarca numerosos temas pero no con mucha profundidad", "se basa en 10 CBK (Common Base Knowledge)", etc.

Pero ¿Cómo es un examen CISSP?.
No son exámenes online. Se establen fechas en distintas partes del mundo y quien está a cargo de tomarlo y monitorearlo es un profesional de seguridad informática que ya posee una certificación CISSP. Existen diferentes fechas para rendir el examen (costo U$S 500). Para ver detalle: www.isc2.org. Pero veamos cuales son los 10 capítulos que componen el CBK y ejemplifiquemos con una pregunta de cada uno de ellos.

Si desea conocer más detalles visite:
http://www.cccure.org/

Este excelente web-site está dirigido por Clement y Nathalie Dupois.

6. Seguridad en las operaciones
La mejor técnica para prevenir y detectar abuso por parte de un usuario con acceso privilegiado es:
A. Buenas Políticas.
B. Revisión por administración.
C. Autenticación fuerte.
D. logs de auditoría.

Respuesta: *B*
Es muy importante el monitoreo por supervisores.

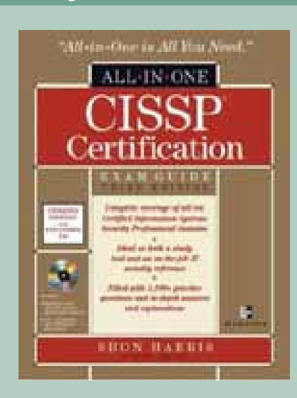
7. Seguridad Física
La seguridad física sigue ¿Cuál de los siguientes modelos?
A. Modelo de defensa de Alta Seguridad.
B. Modelo de defensa basado en disuasión.
C. Modelo de defensa en capas.
D. Modelo de seguridad de sistemas confiables.

Respuesta: *C*

8. Modelos y Arquitecturas de Seguridad.
¿Qué es una vulnerabilidad de un sistema multiproceso?
A. Diferentes niveles de usuarios operando simultáneamente.
B. Ataques a datos sincronizados.
C. Reuso de objetos (object reuse).
D. Insuficiente memoria ram.

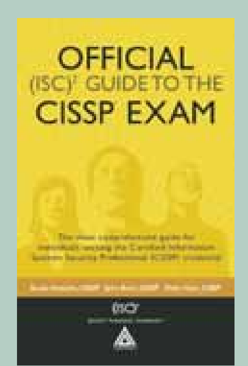
Respuesta: *C*

Mejores **Libros**



CISSP All-in-One Exam Guide, Third Edition (All-in-One) (Tapa Dura)
Autor: *Shon Harris.*

Esta es la tercera edición del libro de Shon Harris considerado el mejor libro para la preparación del examen CISSP. Muchos de sus capítulos han sido renovados usando los comentarios de instructores y estudiante. Al igual que la "Guia oficial"(ver más abajo) es importante complementarlo con más bibliografía. Contiene un CD con un examen de simulación con respuestas y explicaciones.
Nuestra calificación: *9/10*



Official (ISC)2 Guide to the CISSP Exam (Tapa Dura)
Autor: *Susan Hansche*

Esta es la Guia Oficial al examen CISSP autorizado por ISC2. Al ser la guía oficial muestra qué temas se incluyen y cuales no y nos da noción del nivel exacto de las preguntas que componen el examen. Tiene un simulador de examen con preguntas y sus respuesta con explicaciones. Recomendable como complemento al libro de Shon Harris.
Nuestra calificación: *9/10*

4. Criptografía
¿Cuál de los siguientes NO soporta block sizes (tamaños de block) variables?
A. Rijndael
B. RC5
C. Triple-DES
D. Rivest Cipher 6

Respuesta: *C*

5. Leyes, Investigación y Ética
Una organización sospecha que ha sufrido pérdidas debido al accionar malicioso de un empleado. ¿Cuál sería el primer paso relacionado al escenario descripto?
A. Llamar a la policía
B. Despedir al empleado.
C. Establecer capacitación de concientización.
D. Revisar las políticas de la organización.

Respuesta: *D*
Si no hubiese una política clara que dijera explícitamente que se monitorearía la red se recomienda implementarla antes de realizar cualquier acción de sniffing o control del tráfico.

Módulos que componen el CBK:

1. *Access Control Systems and Methodology*
2. *Applications and Systems Development Security*
3. *Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)*
4. *Cryptography*
5. *Law, Investigation and Ethics*
6. *Operations Security*
7. *Physical Security*
8. *Security Architecture and Models*
9. *Security Management Practices*
10. *Telecommunications and Network Security*

9. Practicas de administración de la seguridad.
Integridad es protección de los datos de todos los que siguen EXCEPTO:
A. Análisis de datos
B. Cambios NO autorizados.
C. Cambios accidentales
D. Manipulación intencional.

Respuesta: *A*
Análisis de datos está asociado con confidencialidad y NO integridad.

10. Seguridad en redes y telecomunicaciones
Un datagrama muchas veces contendrá al mensaje más otros headers y trailers. ¿Ésto se llama?
A. Encriptación.
B. Transporte adyacente.
C. Encapsulación.
D. Atenuación.

Respuesta: *C*

¿Qué es el **ISC2**?

Acerca del (ISC)²

El International Information Systems Security Certification Consortium, Inc. [(ISC)²® o también ISC2)] ha establecido un standard muy alto, internacionalmente reconocido, en relación a la educación y certificación de profesionales de seguridad informática.



Fue fundado en 1989 y ha certificado a más de 40.000 profesionales de seguridad informática en más de 100 países. Su base está en Palm Harbor, Florida, USA pero tiene oficinas en Viena, Virginia, USA, Londres, Hong Kong y Tokio. Otorga la certificación Certified Information Systems Security Professional (CISSP), Certification and Accreditation Professional (CAPCM), y Systems Security Certified Practitioner (SSCP) a aquellos que reúnan los requerimientos exigidos. CISSP y SSCP están entre las primeras certificaciones del mundo IT que cumplen los exigentes requerimientos de ANSI bajos estandares ISO/IEC 17024. Este es un marco global para evaluar y certificar personal.
El (ISC)² también ofrece un portfolio de productos y servicios educacionales basados en el CBK. El CBK (Common Base Knowledge) es un compendio de mejores prácticas para profesionales de la industria de la seguridad de la información.
(ISC)² es también responsable del estudio Global Information Security Workforce.

Vea mas sobre (ISC)² en www.isc2.org
Carrera CISSP en www.centraltech.com.ar

TENDENCIAS en desarrollo del SOFTWARE

Con este número iniciaremos una nueva serie: "Tendencias en Desarrollo de Software". La Serie consistirá de 7 artículos redactados por expertos de Snoop Consulting. En este artículo #0 les haremos conocer la Software Development Conference (SD Conference and Expo 2006) analizando las diferentes sesiones (tracks) que la componen. También veremos cómo los artículos propuestos para esta Serie barren muchos temas de los diferentes tracks.

NOTA #0

El negocio del Software:

En este módulo, emprendedores del software y otros profesionales avocados a servicios de software, responderán estas preguntas y más. ¿Qué se necesita para crear, sostener y hacer crecer un exitoso negocio de software.
¿Se imagina como sería comenzar su propia compañía de software? ¿Qué recursos financieros le están disponibles para financiar sus ideas? ¿Cuáles son los asuntos legales, incluyendo open source y patentes, a los que los emprendedores del software se enfrentan? ¿Qué tareas del software conviene terciarizar? ¿Cuáles son las ventajas asociarse estratégicamente?

Justamente, el artículo #1 de esta serie nos responderá estas preguntas en la experiencia de la empresa Snoop Consulting.

#1



Gente, Procesos, y Métodos:

Las técnicas, herramientas e interacciones grupales que logran un exitoso desarrollo de software, pueden variar ampliamente, dependiendo del dominio, tecnología y equipo involucrados.
Aprender habilidades técnicas de alto vuelo, creando procesos efectivos y mantener al equipo de software saludable no ocurre por arte de magia: hay técnicas probadas y herramientas para llegar al éxito. Este track incorpora la última información y las mejores prácticas en métodos ágiles y disciplinados, tips sobre administración de proyectos, desarrollo del grupo, y más.

#2



Modelado y Diseño:

Un software exitoso es directamente atribuible a un elegante y eficiente modelado y diseño. Los modelos permiten a los desarrolladores construir una entendible representación visual de sistemas orientados a objetos antes de zambullirse en el código fuente. Este track incorpora la última información y mejores prácticas incluyendo, pero no limitándose a UML, arquitectura de software, patrones de diseño, análisis de robustez, y diseño de base de datos.

#3

#7

Servicios Web:

Ahora que el mundo está interconectado, las computadoras hoy pueden rutear inteligentemente y administrar la información que es enviada a través de Internet en forma de Web Services. El track de Servicios Web, explica y explora los conceptos y tecnologías que permiten la comunicación de una computadora a otra. Estándares como SOAP y UDDI serán tratados y cada uno será aplicado a tecnologías como Oracle, J2EE o Apache. Los asistentes aprenderán las bases, plataformas y estándares de Web Services y cómo aplicarlas a su ambiente IT.



Seguridad:

La seguridad de las aplicaciones es esencial en el mundo de hoy, y este track de seguridad muestra como construirla desde cero. Hace foco en los desafíos y soluciones de seguridad de las aplicaciones, permite entender las más recientes tendencias y desarrollos en la industria, y compartir conceptos para fortalecer las aplicaciones así como las capacidades de programación. La seguridad es más importante que nunca, y los retos para resguardar los sistemas son cada vez más complejos. Ya sea que uno se responsabilice por uno o cientos de sistemas, los cursos de este track proveerán de información esencial para ayudar a estar al día con las últimas amenazas e implementar poderosas herramientas y técnicas para mantener los sistemas seguros.

Requerimientos y análisis:

Lograr un software exitoso es directamente atribuible a entender bien requerimientos para cumplir con los requerimientos de los consumidores. Para tener éxito se necesitan técnicas que facilitan las comunicaciones entre clientes y desarrolladores en el espíritu de aprender y descubrir. Este track incorpora la más reciente información y mejores prácticas como ser recopilación de requerimientos, modelado ágil, casos de uso, reglas de los negocios, modelado de negocios, análisis centrado en el usuario, y análisis de robustez.





Testeo y Calidad:

¿Cómo saber si nuestro software funciona? ¿Cómo saber si fue programado apropiadamente? ¿Deberíamos si quiera preocuparnos? Este track explora técnicas de avanzada para testeos y Quality Assurance que pueden ser usadas en situaciones reales.

#4



Desarrollo en .NET:

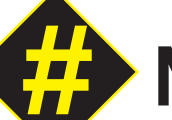
Desde su debut hace 6 años hasta su segundo lanzamiento el año pasado, .NET se ha establecido como una plataforma de desarrollo predominante, con las mejores herramientas y soporte para tecnologías emergentes y nuevos estándares, desde Indigo y Avalon a Smart Clients y programación clásica de sistemas. El track de .NET de este año tiene tres temas: el primero es una presentación en profundidad de las nuevas características y capacidades de .NET 2.0, desde la estructura de las aplicaciones, hasta los lenguajes y Visual Studio; y el segundo es su aplicación exitosa: el track incluirá sesiones .NET en proceso de desarrollo, ideas que permiten la productividad, técnicas, interoperabilidad con código "anterior" (legacy) y otras plataformas, y el tercer tema son las tendencias tales como Smart Clients, Avalon e Indigo.



Programación Java:

Java continúa siendo el lenguaje de programación dominante para la creación de aplicaciones basadas en la Web. Dominar Java en profundidad significa entender muchos detalles del lenguaje, en particular, las poderosas características y bibliotecas que diferencian a Java de sus predecesores.

#5



NOTAS



- #1 El negocio del Software: Caso de Éxito Snoop Consulting



- #2 Métodos ágiles y disciplinados



- #3 Modelado y diseño de sofware



- #4 Quality Assurance de Software
- #5 JAVA vs. .NET
- #6 Data Warehouse, Bussiness Intelligence y Data Mining
- #7 Coordinando procesos de negocios con BPEL

La Software Development Conference reúne a los visionarios y los más expertos en la industria para informar a los participantes de las tendencias y novedades que les depara el 2006.

La SD Conference es la más grande y concurrida conferencia de software independiente, con más de 150 expositores. Con un enfoque en programación y desarrollo de aplicaciones y tendrá lugar durante marzo 2006 en Santa Clara California. Durante esos días se dictarán más de dos centenares de clases de entrenamiento sobre Java, C++, UML, usabilidad y desarrollo de Internet/Intranet, middleware, COM, CORBA, y asuntos administrativos. Dictadas por destacados autores y desarrolladores.

Todos los principales players de la comunidad de desarrolladores se congregan anualmente para desarrollar una currícula de eventos que combina lo mejor de la programación, tanto tradicional



como de la próxima generación, en un lenguaje y un ambiente de plataforma neutrales. Cubren todos los temas, como C++, JAVA, XML, Servicios Web, Seguridad y otros.

Cuenta con importantes auspiciantes, como corporaciones de la talla de IBM, Microsoft, Amazon, la IEEE Computer Society, entre muchos otros.

Pero analicemos los "tracks" (sesiones) en las que se divide la reunión de modo de entender hacia donde se dirige el mundo de la programación y veamos cómo se realacionan con los artículos que propusimos para esta Serie.

Una segunda serie de artículos abarcará temas como Seguridad, Lenguajes, C++, XML...

C++:

C++ se ha usado comercialmente de forma muy difundida por más de una década, sin embargo todavía los programadores continúan encontrando formas innovadoras de usar el lenguaje y sus librerías estándar. C++ continúa teniendo un montón de sorpresas interesantes. La existencia de esta session nos muestra cuán vigente es aun hoy C++.

La evolución de XML:

En un tiempo relativamente corto, XML se ha convertido en la lengua franca del desarrollo basado en la Web; pero XML también tiene aplicaciones mucho más allá de la Web, como formatos de archivo personalizados, desarrollo de componentes de software, e integración de base de datos. XML provee un mecanismo común para compartir información entre aplicaciones, así como mecanismos comunes de representaciones de datos en los que todos pueden estar de acuerdo. Elegir XML clarifica los datos, los hace más fáciles de procesar y más flexibles frente a cambios inesperados y cambios en los requerimientos. El track de XML cubre todas las facetas del XML y sus aplicaciones relacionadas desde un nivel introductorio hasta el límite de lo complejo.

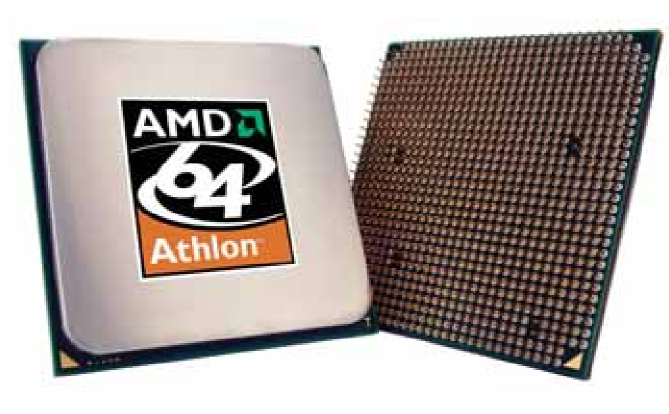
Los temas de interés que incluye son:

- XSLT
- JAXP
- SAX
- DOM
- Esquemas
- XForms
- Web Semántica
- Bases de Datos XML Nativas
- XQuery
- Atom



Servers en **PyMEs** y **Corporaciones**

Nota 1 de 2:
"PyMEs"





Maximiliano Di Toro
Network Adminstrator

Para satisfacer la demanda que una red típica de una Pyme, puede resultar más que suficiente una PC de escritorio que esté a la altura de un Server corporativo en materia de prestaciones, pero con costos acordes a un presupuesto moderado, y que se adapte a las necesidades y requerimientos de la pequeña y mediana empresa.

Para satisfacer la demanda que una red típica de una Pyme, puede resultar más que suficiente una PC de escritorio que esté a la altura de un Server corporativo en materia de prestaciones, pero con costos acordes a un presupuesto moderado, y que se adapte a las necesidades y requerimientos de la pequeña y mediana empresa.

Cuando uno destina un presupuesto a una computadora a la que le dará un uso exclusivo como Servidor, no es necesario pensar una súper-computadora, sino que las funciones críticas que típicamente realizará tienen que ver con transferencia de archivos, administración de permisos, o ser un "semáforo" en el tráfico dentro de la red. Para aquellas funciones los componentes de hardware que más influirán serán el microprocesador, los discos rígidos, memorias, y por supuesto las placas de red. Comencé con un motherboard "hogareño", pero de alta gama, que tiene una excelente performance si se lo acompaña de una buena combinación de memoria, micro y discos. El **Asus A8N - E**, a éste le agregamos un microprocesador **AMD Athlon 64 3500+** BOX (Socket 939) que cuesta unos U$S 260, una placa de video X300SE 256Mb PCI EXPRESS U$S 79, 2 módulos de memoria Ram PC 3200 de 1Gb cada uno por U$S 220 el par, 2 discos rígidos Western Digital de 160 Gb SATA II en RAID a unos U$S 250, una Regrabadora de DVD Pionner 16X Dual Layer U$S 65 un Gabinete con una fuente Satellite 535 de 400W Reales a U$S 120 y un monitor Samsung 793S de 17 pulgadas, ¿Por qué 17 pulgadas? Por la diferencia monetaria casi inexistente que hay entre un monitor de 15" y uno de 17" no vale la pena ahorrar U$S 10 ya que si en algún momento de urgencia necesitamos un monitor podremos disponer el del servidor ya que éste no se debería usar para ninguna otra tarea a menos que sea indispensable, o bien usar el de 17 en alguna PC cliente y en el Server usar el que anteriormente tenia la cliente.

Asus A8N - E:
- Front Side Bus de 2000/1600 MT/s.
- 1 Slots PCI Express 16X
- 1 PCI Express 4X
- 2 PCI Express 1X.
- 3 Puertos PCI.
- Memoria RAM: 4 DIMM DDR 400/333/266 Arquitectura Dual Channel.
- nForce4: 4 x SATA 3Gb/s.
- NVRAID: RAID0, RAID1, RAID0+1 y JOBD span cross SATA y PATA
- 2 x UltraDMA 133/100/66/33
- Controlador de red 10/100/1000Mbps: Force4 built-in Gbit MAC con external Marvell PHY.
- NV ActiveArmor Firewall y otra gran cantidad de características.

Para los que prefieran **Intel** se puede armar una PC basada en el mejor motherboard de Intel: el **Intel D975XBX** por U$S 275, junto a un microprocesador **Intel Pentium 4 630** con 2Mb de caché L2 de 64 Bits BOX (Socket 775) a U$S 250, Memoria RAM: 2Gb DDR2 533Mb (2X1GB) Dual Channel por U$S 220, 2 discos rígidos Western Digital de 160 Gb SATA II en RAID a U$S 250 ambos, una placa de video X300SE 256Mb PCI EXPRESS, una Regrabadora de DVD Pionner 16X Dual Layer U$S 65, un Gabinete con una fuente Satelite 535 de 400W Reales a U$S 120 y un monitor Samsung 793S de 17 pulgadas.

Intel D975XBX :
- 2 Slots PCI Express 16X
- 1 PCI Express 4X
- 2 Puertos PCI.
- Memoria Ram: Cuatro sockets DDR2 SDRAM DIMM, hasta 8 GB totales.
- Sonido Integrado: Intel® High Definition Audio subsystem.
- Red: Gigabit (10/100/1000 Mbits/sec) LAN subsystem usando el Intel® 82573E/82573L Gigabit Ethernet Controller.
- 8 Puertos USB 2.0
- Chipset: Intel® 975X Express.
- Discos: Cuatro interfaces Serial ATA con soporte RAID.
- Una interfaz Parallel ATA IDE con soporte para UDMA 33 y ATA-66/100.
- Video: Dos conectores PCI Express x16, (uno Primario y otro conector Secundario).

Software

Lo primero a definir es el sistema operativo, sobre el cual correrán los programas que utilicemos, que dependerán de cual sea la especialidad de nuestra empresa.

Dentro de la reducida variedad de Sistemas Operativos (SO), al menos apropiados para un servidor, se puede optar por uno de los más difundidos como ser **Microsoft Windows Small Business**

Server 2003 Premium 64 Bits cuyo precio estimado es de unos U$S 1410 (Microsoft Small Business Server 2003 Edición Premium incluye: Windows Server 2003 con servidor de fax, seguridad, comunicaciones y sitios Web internos; correo electrónico, mensajería y colaboración con Exchange Server 2003 y Microsoft Outlook 2003; base de datos con Microsoft SQL Server 2000; seguridad avanzada con Microsoft Internet Security and Acceleration (ISA) Server 2000; desarrollo de sitios Web con Microsoft Front Page 2003 y otras aplicaciones exclusivas, e incluye 5 licencias de acceso de usuarios), con el cual aprovecharemos a fondo nuestro procesador de 64 bits y la memoria en 128 bits debido al dual channel. Si bien no hay aún las suficientes aplicaciones preparadas para explotar los 64 bits muy pronto estarán disponibles y es mejor estar preparados. A ésto le podemos agregar un Microsoft Office 2003 Pyme a U$S 295.
Otra opción a tener en cuenta es el **SUSE LINUX Enterprise Server 9** X86 AMD64 e Intel EM64T la cual es una versión paga de Linux desarrollada por Novell, que se adapta de manera muy eficiente a las necesidades de una mediana empresa. Por casi U$S 350 podremos contar con la version completa que incorpora el paquete de **Open Office.org** el cual incluye el Writer (un avanzado procesador de textos), Calc (planilla de cálculo), Impress (presentaciones visuales), Draw (organigramas, gráficos vectoriales), Math (editor de ecuaciones y fórmulas) a los que se agrega Base (data base).
Por otro lado tenemos a **Red Hat Enterprise Linux ES** en su versión básica por U$S 350 la cual esta a la altura de las necesidades soportando tanto los microprocesadores de AMD e Intel de 64 Bits y brindando una muy buena compatibilidad y aprovechamiento de la tecnología de 64 bits.
También podemos optar por una de las tantas distribuciones gratuitas de Linux y bajar el paquete Open Office.org; ambos son open source y gratuitos.
La decisión de ahorrar costos utilizando un sistema operativo gratuito (Linux), o ir a lo seguro y adquirir una licencia paga de uno open source (SUSE o Red Hat) o por un monto a penas mayor elegir un SO que prácticamente es un estándar en las PC actuales (Windows), queda a total discreción de la empresa, y tendrá que tomar en consideración factores como la capacitación de su Network Administrator, cantidad de terminales conectadas a su red, y la compatibilidad de soluciones de seguridad de terceros previamente instaladas en la red.

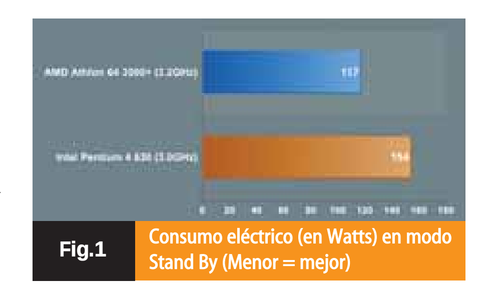
Consumo de Energía
En un principio, la performance de los microprocesadores estaba basada netamente en su cantidad de ciclos por segundo, luego AMD comenzó a fabricar micros con cada vez más rendimiento por ciclo individual, por lo que comenzó a nombrar a sus modelos con la performance equivalente a su competidor, en lugar de indicar la velocidad de reloj propia. Por ejemplo un microprocesador AMD Athlon 64 3500+ trabaja a una frecuencia de 2200MHz, mientras que un Intel Pentium 4 630 lo hace a 3000MHz. Y aunque el micro de AMD funcione a una velocidad 27% menor que el de Intel, ambos rinden de forma semejante.
La compra de un CPU es una inversión, y en lo que a la ésta se refiere, el consumo de energía del microprocesador es cada vez más importante. Así como uno no deja prendidas la luces al retirarse de una habitación, ya que el sentido común nos lleva a apagarlas y ahorrar energía cuando no están en uso; Pues de igual manera, el microprocesador debe tener apropiadas políticas de restricción del uso de la electricidad cuando no la emplea.
Así mismo, cuando uno compra un microprocesador, puede resultar de particular interés contemplar su velocidad en relación a los Watts de potencia consumidos.
En ciertos casos el costo de la corriente que alimenta al CPU puede eventualmente superar el costo de la adquisición del mismo.
En esta materia, una de las innovaciones que presentan los AMD en su arquitectura K8 es la reducción de la escala de sus circuitos a 90nm (nanómetros), lo que, a parte del lógico incremento de su performance, le permite alcanzar picos de trabajo consumiendo cantidades mucho menores de electricidad. Como muestra de este avance, los números que los benchmarks muestran son más que evidentes: un AMD Athlon 64 3500+ funcionando a toda máquina consume mucha menos electricidad que un Pentium 4 630 a 3000MHz en stand by (Fig 1 y 2).

Performance en Aplicaciones Ofimáticas
Empleando el benchmark Winstone pusimos a prueba el desempeño al ejecutar los más comunes softwares instalados en oficinas y servidores (Fig.3):

Microsoft Access 2002
Microsoft Excel 2002
Microsoft FrontPage 2002
Microsoft Outlook 2002
Microsoft PowerPoint 2002
Microsoft Project 2002
Microsoft Word 2002
Norton AntiVirus Professional Edition 2003
WinZip 8.1

Los Athlon se lucen más durante la ejecución dedicada a una aplicación en particular. En los siguientes test veremos si Intel logra ponerse a la altura de su competidor cuando se los pone a prueba.

Productividad en la Oficina
A continuación vamos a ejecutar el benchmark de Productividad en la Oficina de **SYSMark 2004**, a lo largo del cual someteremos a los microprocesadores a tres test, el primero de los cuales refiere a las Comunicaciones. El procedimiento del test es el siguiente:
"El usuario recibe un e-mail en Outlook 2002 conteniendo una serie de documentos comprimidos dentro de un archivo Zip. El usuario lee dicho e mail y actualiza su calendario mientras el VirusScan 7.0 escanea su sistema. El website de su empresa es visitado en Internet Explorer 6.0. Finalmente dicho navegador es utilizado para visualizar los documentos creados durante este Test." (Fig.4).


Fig.1 Consumo eléctrico (en Watts) en modo Stand By (Menor = mejor)

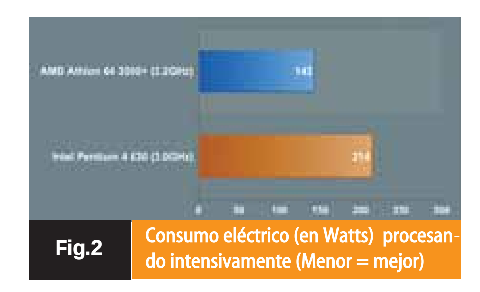
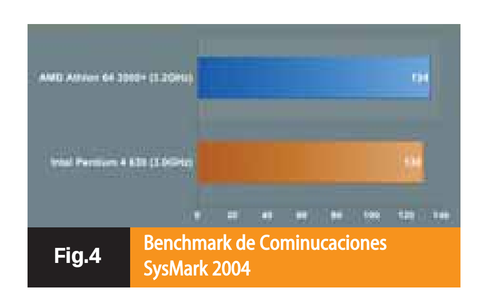

Fig.2 Consumo eléctrico (en Watts) procesando intensivamente (Menor = mejor)


Fig.3 Performance en Aplicaciones Ofimáticas Business Winstone 2004


Fig.4 Benchmark de Cominucaciones SysMark 2004

El segundo test de la serie consiste en medir la Performance en la creación de Documentos.
Éstos son los pasos que sigue el test:
"El usuario edita un documento usando Word 2002. Luego, transcribe un archivo de audio en un documento usando el Dragon NaturallySpeaking 6. Una vez que el documento está completo, se lo transforma a formato PDF usando el Acrobat 5.0.5. El usuario crea una presentación de marketing en PowerPoint 2002 y agrega elementos a una plantilla de presentación." (Fig.5 en próxima página).



El tercer y último test consiste en el Análisis de Datos, que se desarrolla de la siguiente manera: *"El usuario abre una base de datos usando Access 2002 y ejecuta algunas consultas. Un conjunto de documentos es comprimido usando WinZip 8.1. Los resultados de las consultas son importados en una hoja de cálculo usando Excel 2002 y son usadas para generar gráficos" (Fig.6).*

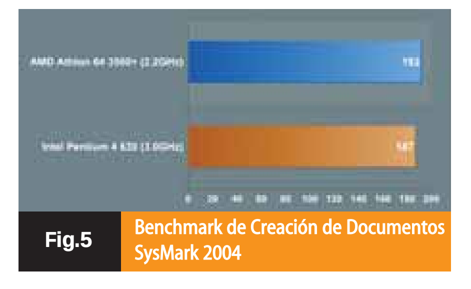


Fig.5 Benchmark de Creación de Documentos SysMark 2004

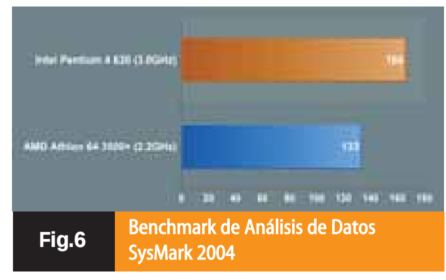


Fig.6 Benchmark de Análisis de Datos SysMark 2004

Rendimiento en Multitareas

En este examen analizamos la performance al realizar múltiples procesos en simultáneo:

En el gráfico veremos como se desempeñan al comprimir un archivo de 130MB, a la vez que paralelamente se importa un archivo PST de 260MB de Outlook 2003. Durante la ejecución, estarán abiertos el Firefox y el iTunes.

La cantidad de segundos indicada en el gráfico marca los siguientes parámetros: cuánto le llevó al WinRAR comprimir el archivo, y la cantidad de e-mails importados en dicho lapso; a menor tiempo, mejor (Fig.7).

Si bien hasta ahora, la performance de ambos es pareja en los tests de multitarea.

Veremos si al realizar operaciones más avanzadas y complejas alguno de los dos toma la delantera.

Como prueba final de esta comparativa, realizaremos el test de multitarea que incluye el **Business Winstone 2004**, que realiza en lo siguiente:

Este test usa los mismos programas que el test de Performance en Aplicaciones Ofimáticas, pero ejecuta algunas de éstas en segundo plano. El test consta de tres segmentos: el primero de éstos copia archivos en segundo plano mientras ejecutamos el Microsoft Outlook e Internet Explorer en primer plano. El benchmark espera que las anteriores tareas se completen antes de comenzar el segundo segmento. En ese segmento, Excel y Word se ejecutan en segundo plano mientras WinZip comprime en segundo plano. Una vez que todo lo anterior ha finalizado, comienza el último segmento. En éste, el Norton AntiVirus realiza un escaneo del sistema en segundo plano, mientras el paquete completo de Office 2002 más el Microsoft Project y WinZip corriendo en segundo plano (Fig.8, 9, 10 y 11).

Después de haber visto la comparativa entre dos equipos con similares características en configuración de memoria, discos, etc, con la sola diferencia de los microprocesadores, queda a su criterio la elección que más se adecúe a su empresa. Pese al precio inferior de los microprocesadores de 32 bits, se justifica la compra de alguno de estos dos modelos de microprocesadores de 64 bits ya que su performance es mucho mayor que la de los 32 bits y se notará cada vez más la diferencia en el futuro, a medida que las aplicaciones comiencen a aceptar instrucciones en 64 bits.

AMD tiene como punto negativo la imposibilidad de llegar a los 8 Gb de RAM ya que ninguna placa madre soporta tal suma. ■

	AMD	Intel
Mother	$ 160	$ 299
Micro	$ 259	$ 250
Memoria Ram	$ 220	$ 220
Disco Rígido	$ 250	$ 250
DVD	$ 65	$ 65
Placa Video	$ 79	$ 79
Gabinete/Power	$ 125	$ 125
Monitor	$ 112	$ 112
Total	**$ 1.270**	**$ 1.400**

Precios expresados en Dólares americanos

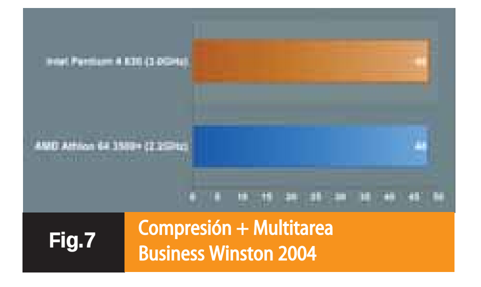


Fig.7 Compresión + Multitarea Business Winston 2004

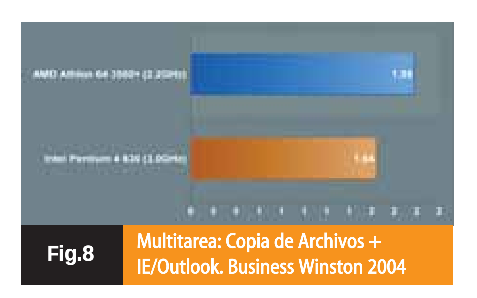


Fig.8 Multitarea: Copia de Archivos + IE/Outlook. Business Winston 2004

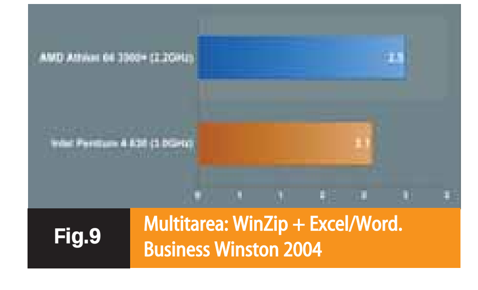


Fig.9 Multitarea: WinZip + Excel/Word. Business Winston 2004



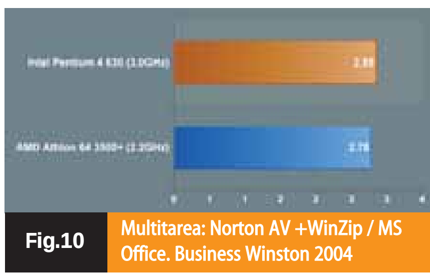


Fig.10 Multitarea: Norton AV +WinZip / MS Office. Business Winston 2004

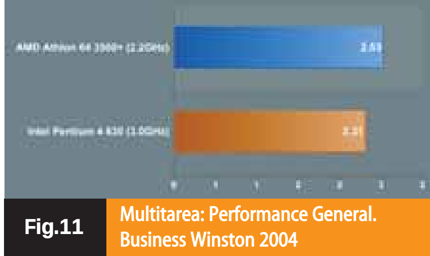


Fig.11 Multitarea: Performance General. Business Winston 2004



El desafío de las **Nuevas Tecnologías** y regulaciones en la **Empresa**

David A. Yanover
Director de www.MasterMagazine.info

Sarbanes Oxley, ISO 17799 / 27001, ITIL, ISACA, ISC2, HIPAA... El mundo de los negocios se ve ante la necesidad continua de estar al día con respecto a los últimos desarrollos tecnológicos, para enfrentar a la competencia. Pero también, se debe ser conciente de las formas correctas de aplicación de sistemas informáticos, para que la tecnología no se convierta en un problema.

La tecnología aplicada sobre el modelo de negocios de una empresa, sin importar el ámbito en el cual se desempeñe, es uno de los mayores desafíos del mercado actual, donde cada compañía debe saber como marcar la diferencia, para así destacarse sobre el resto.

Hoy, pensar en tecnología significa pensar en mejorar la producción, los contactos de trabajo, ahorrar tiempo optimizando y automatizando ciertas actividades. Pero al mismo tiempo, el cambio en el ambiente de trabajo generado a partir de la inclusión de nuevos parámetros laborales, que podría describirse como una "actualización", obliga a una re-adaptación de los modelos de negocios. Adquirir y aplicar soluciones tecnológicas que ayuden a desarrollar una infraestructura interna más sólida, es un proceso que debe estar acompañado por la gente que en última instancia la pone en práctica.

Más allá de la virtualidad de Internet y de las herramientas informáticas, aparece una continua necesidad por trascender los límites de los bits, para luego volver a digitalizar el mundo incorporando nuevas informaciones. Internet es el mundo de mayor dinamismo que, en convergencia con los modelos de negocios tradicionales, puede propiciar nuevas oportunidades y agilizar drásticamente cualquier tipo de tarea. Incluso, estamos en un siglo en el que pueden reconocerse tanto empresas que sitúan la mayor parte de su infraestructura sobre bases "físicas" como compañías que establecen sus edificios dentro de términos virtuales.

Convergencia de dos mundos

Aprovechar los beneficios de ambos mundos puede generar, al mismo tiempo, grandes problemas. La dependencia es una pauta que debe analizarse; ¿Qué medidas tomar ante una eventual caída del sistema, que puede ocasionar pérdidas económicas y un deterioro en la imagen ante los clientes? Igor Sas, Presidente de Data Express, empresa dedicada a proveer respuestas ante emergencias de continuidad de negocios, explica que "el mayor riesgo es la soberbia de pensar 'a mi no me puede pasar'. Lamentablemente siempre que sucede una contingencia, ésta aparece por el único lugar que dejamos sin cubrir. Es sorprendente la cantidad de recursos que tiene la fatalidad, el descuido, la desidia, y otros detalles para generar eventos que pueden terminar en diferentes grados de emergencias".

Pero tampoco hay que caer en el otro extremo, dejándose llevar, sin ir más lejos, por el miedo que impulsan muchos analistas alrededor del concepto del ciberterrorismo. Sobre esto último, consultamos a Ignacio Sbampato, Vicepresidente de Eset Latinoamérica, quien advierte que el término está siendo promovido de tal manera que cause una paranoia en la sociedad. "A lo que se refiere el ciberterrorismo, del modo en el que se lo está impulsando, es a la gran cantidad de troyanos, spam y gusanos que hay en Internet. Ésto no es terrorismo bajo ningún punto de vista, sino que se trata de estafas, porque detrás de estas acciones hay, por ejemplo, personas que pagan por el envío de spam o individuos que construyen redes de

PC's zombies para alquilarlas al mejor postor. En resumen, no tiene nada que ver con el terrorismo, que hasta donde yo se, significa causar terror con fines políticos o religiosos". De hecho, numerosos estudios revelan que las amenazas en las infraestructuras tecnológicas se aprecian con más frecuencia dentro de la propia empresa; un mal uso de las políticas de seguridad puede ser mucho más peligroso que un virus.

Para Marcelo Lozano, Business Development Manager de Patagonia Technologies, "la complejidad en si misma no radica en la tecnología, sino que es propia del modelo de negocios y el marco económico que en conjunto conforman un sistema caótico. La tecnología juega el rol de atractor, siendo el medio ideal y necesario para poder administrar el negocio en un entorno desorganizado. Desde la caída del muro de Berlín algunas reglas cambiaron para siempre el mundo de los negocios". Conversando con el experto, se identificaron una serie de aspectos, analizando el tiempo en el que vivimos:

- *Las tecnologías de las comunicaciones barrieron el tiempo y las distancias.*
- *La economía se globalizó, aumentando el número de clientes, pero también de competidores .*
- *Las nuevas industrias cambiaron el paradigma de la infraestructura por el de la innovación.*
- *Enormes flujos de capitales disponibles.*

Es una realidad: el propio mercado ha marcado la necesidad para las empresas de animarse a probar nuevas tecnologías. Sin embargo, aún muchas instituciones públicas y privadas muestran un cierto rechazo hacia este tipo de implementaciones, porque no comprenden sus ventajas, y es por eso que su aplicación termina en un caos. Hay que capacitarse, hay que saber lo que se está adquiriendo, ya sea analizando la situación por medio de un departamento especializado en el área TI o consultando con los propios proveedores de los servicios tecnológicos.

Pensemos por un momento en el uso cotidiano de la PC, -en sus diversas formas según el usuario que la está utilizando-. Un diseñador gráfico que trabaja con avanzados y pesados programas de imagen y video; un joven amante de los videojuegos que tiene la computadora para divertirse en sus ratos libres; un CIO que lleva adelante intensos análisis del estado de producción de la empresa, trabajando con aplicaciones de planeamiento ERP; un programador, encargado del desarrollo de aplicaciones internas, haciendo uso de software especializado. Las posibilidades y el potencial de las herramientas informáticas que se presentan cambian según el usuario, y sin embargo la PC continúa siendo la misma. La magnitud de una modificación en las políticas de trabajo de una empresa supera ampliamente al uso de la PC particular de cada persona, porque es un cambio que la afecta a nivel general y los usuarios deben estar preparados, para poder aprovechar todo el potencial que es capaz de generar una solución tecnológica.

En este sentido, surgen una serie de prácticas, certificaciones, leyes gubernamentales y estándares que marcan e identifican el buen uso de la tecnología en la empresa.



ISO 17799-27001: una Constitución dentro del ámbito de la seguridad digital

Consiste en una serie de pautas recomendables de seguridad, que comprende profundos niveles de protección de la empresa, a la que considera como una totalidad. Es un estándar internacional

IEC

que cubre todos los aspectos a tener en cuenta en la seguridad de la compañía. Originalmente, apareció BS 7799 (estándar para la gestión de la seguridad de la información) que luego se transformó en ISO 17799 (code of practice information security management).

Lo que establece ISO 17799 son guías de pasos a seguir ante eventuales problemáticas afrontadas en la empresa; situaciones críticas que se relacionan con las políticas de seguridad, aspectos organizativos, la seguridad del personal, la clasificación y el control de los activos, la protección física y propia del ambiente de trabajo, la producción y el mantenimiento de los sistemas, el control de accesos, la continuidad de los modelos de negocio, y también, el entorno legal con respecto a la seguridad y la empresa a nivel general.

La empresa Argentina de seguridad Etek logró obtener la revalidación de ISO 17799/BS 7799, a lo que Juan Carlos Vuoso, Gerente General de ETEK Argentina, explica que ello "consolida nuestra imagen frente a los clientes y avala nuestra capacidad para atender los aspectos referidos a la seguridad de la información. Fue un compromiso estratégico alineado con la misión que tiene la empresa. Nuestro primer desafío fue alcanzar la certificación según ISO 9001 para todos los procesos operativos relacionados con nuestros servicios y soluciones". Le preguntamos sobre las implicaciones que tiene una firma como ésta, a lo que Vuoso puntualiza que "cuando se analizan las razones de la adopción de la norma BS7799, se comienza considerando fundamentos directamente relacionados con la infraestructura tecnológica. La estrategia de seguridad que se implementa en una empresa es en realidad un sistema que, en forma bien simplista, se asocia con los recursos tecnológicos que se van incorporando para atender a requerimientos específicos: antivirus, firewall, filtrado de contenido, etc. Aplicando la analogía de la cadena, el sistema será tan fuerte como el eslabón más débil. Para evitar puntos débiles es apropiado adoptar un criterio que permita enfocar al sistema como un todo. La adopción del Framework o infraestructura de criterios que recomienda la norma ayuda a optimizar este sistema".

"Las personas constituyen un eslabón dentro del sistema o cadena que se mencionó antes -muchos opinan que es el más débil-. La ISO promueve el establecimiento formal de procesos y controles que a la vez de facilitar el desenvolvimiento de los empleados en la forma apropiada, también brinda una herramienta para detectar y resolver desviaciones en esos procesos, antes que sea demasiado tarde. La adopción de la norma ayuda a definirlos en forma precisa". No se trata sólo de un respaldo hacia la imagen de una empresa, sino que se gana experiencia de mucho valor aplicable de manera directa sobre el proceso de negocio.

Pensar en la compatibilidad de los distintos estándares que se desarrollan a partir del uso de las aplicaciones que componen la infraestructura tecnológica de la empresa es precisamente donde se manifiestan las prácticas de ISO 17799, para que las cosas funcionen sin sorpresas.

Para explorar a fondo esta certificación, se consultaron varios documentos desarrollados por la firma de análisis Forrester, que revelan ciertos aspectos en los que ISO/IEC tuvo que trabajar para estar a la altura de las circunstancias. Tal es el caso de la falta de atención que se le dedicó a los factores de riesgo en la primera versión de ISO/IEC 17799, y que luego de una revisión logró complementarse con información concreta acerca de determinadas acciones administrativas. También, se le dio un espacio a los incidentes de gestión; y la integración con otros estándares ISO a partir de la revisión fue otro importante avance que proporcionó un panorama más amplio y prometedor. Un claro exponente de cambio generacional tecnológico, y que ha sido tenido en cuenta en la información registrada por la certificación, ha sido la informática móvil, que actualmente resulta indispensable en muchos procesos de trabajo.

Hay que advertir que la ISO 17799 no es certificable por sí sola, sino que se limita a desarrollar Mejores Prácticas. De esta forma, está complementada con BS 7799-2 (la cual sí es certificable). Éste último, fue reemplazado por la ISO 27001 el pasado octubre, la cual lleva los estándares a nuevos niveles, exponiendo un Sistema de Seguridad de la Información Continuo. El ISO/IEC ISO 27001 (que tiene sus siglas a partir de ISO -International Standards Organization- e IEC -International Electrotechnical Comission-) es la última entrega de un desarrollo en constante evolución, siguiendo los cambios propios del sector tecnológico y las necesidades de las empresas.

La guía de seguridad más importante hoy en día en el mundo encontró en sus comienzos el rechazo de seis miembros de G7; el único que lo apoyó fue aquél que lo vio nacer, Inglaterra.

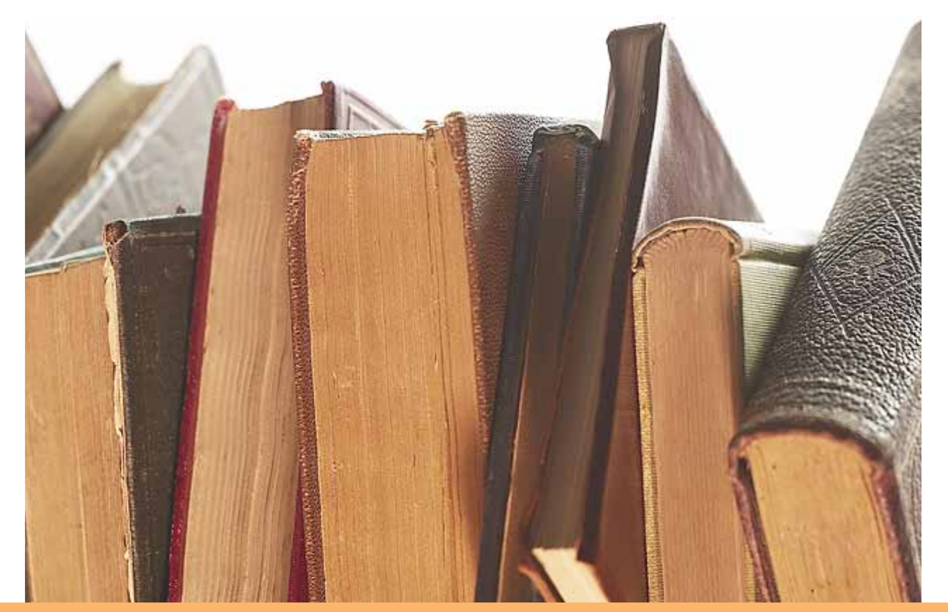
ISO/IEC 17799 es el origen de la madre de las normas en seguridad informática. Su implementación mundial y su constante evolución y proyección a futuro son una garantía para una empresa que quiere pensar en el mañana.



Sarbanes Oxley: ¡Cuidado! Estados Unidos está haciendo controles financieros

Luego de las polémicas caídas de los gigantes Global Crossing, WorldCom y Enron, en los que las compañías estaban sobrevaluadas y las cifras de sus acciones subían sin justificación, las regulaciones y el control sobre las empresas norteamericanas se transformó en uno de los focos de atención. Se había generado una crisis a raíz de los fraudes cometidos. Fue en el 2002 cuando el gobierno presidido por Bush aprobó Sarbanes Oxley (presentada por los congresistas Paul Sarbanes y Michael Oxley), una ley que exigía una serie de informaciones financieras a aquellas empresas que operaban en la bolsa de Estados Unidos. La fecha límite para estar al día con respecto a estas demandas es el próximo 15 de julio (lo cual es una expansión de un año sobre el plazo original). ¿Qué es esta regulación? ¿Cómo han respondido hasta ahora los mercados? Son inquietudes normales para un CEO, y sobre las cuales se ha orientado este capítulo de la investigación sobre el uso de la tecnología y las reglas de juego en la empresa actual.

Los principales aspectos que conforman la ley se aprecian en tres apartados. La Sección 302 solicita que el Director General y el responsable



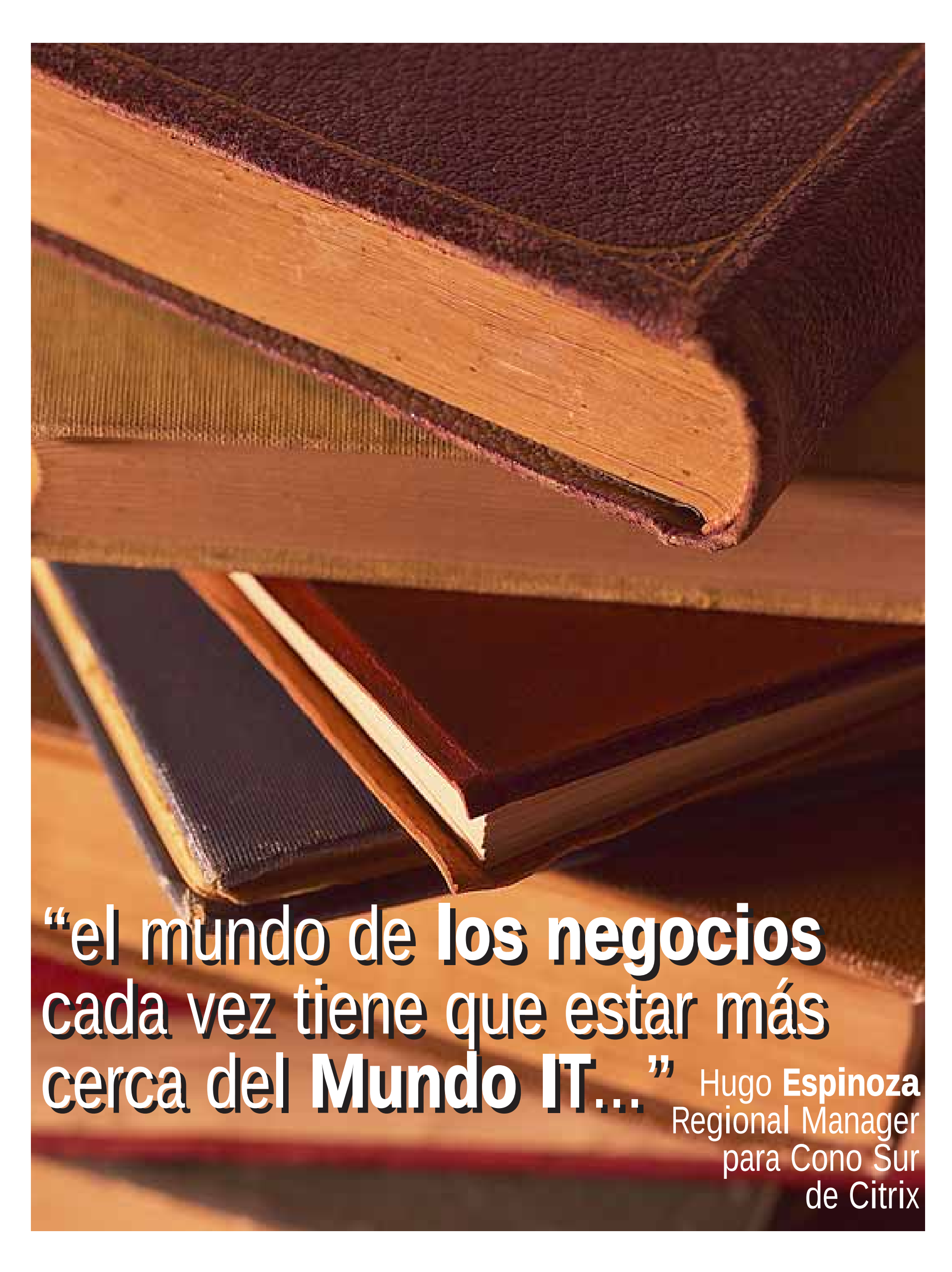
Financiero certifiquen la validez de los informes trimestrales de la compañía. Por su parte, la Sección 404 requiere la documentación de los procedimientos y actividades, en relación a la elaboración de los reportes financieros. Los mismos deben ser aceptados por una firma de auditoría independiente, y paralelamente, todos los documentos y acciones deben ser almacenados digitalmente durante seis años para su fácil acceso. Mientras que la Sección 409 completa el aparato de monitoreo, en cuanto a la disponibilidad y al modelo de registro de los datos, exigiendo a las empresas que identifiquen en tiempo real los cambios en sus operaciones. Básicamente, la ley proyecta la realización de detallados informes financieros, advirtiendo todas las actividades para luego ser auditadas con el objetivo de lograr un mercado transparente.

Paradójicamente, se ha creado un nuevo mercado en torno a la ley Sarbanes Oxley, porque empresas como Oracle o Sun desarrollaron soluciones que automatizan los rigurosos y tediosos procesos de control, que se convierten en un gasto importante para las compañías. Estar conforme a las normas de esta ley no es una opción, sino un requisito, y muchos profesionales creen que están pagando por lo sucedido años atrás con el caso Enron; y están pagando altos precios, reflejados en consultoría, software, y tiempo de un personal que no está capacitado inicialmente.

Según una encuesta de Akonix Systems, el 45% de los ejecutivos IT no espera alcanzar la exigencia de retención de mensajes conforme a la sección 404 (haciendo referencia a la disponibilidad y al registro de la información). El 29% de los 157 profesionales consultados cree que logrará dicha demanda para la segunda fecha límite de la ley (que recordemos, debió moverse un año, a julio de 2006), mientras que el 26% no sabe si estará listo. Francis Costello, Director de Oficina de Tecnología de Akonix, cree que el estado de las cosas es alarmante. "Los negocios deben darse cuenta de que por no registrar y archivar todas las comunicaciones electrónicas, incluyendo aquellas de mensajería instantánea (IM), puede resultar en la obligación legal corporativa. Las demandas de agencias regulativas incentivan a las organizaciones a revelar regularmente las políticas en torno a la administración de correo electrónico y servicios de IM, pero muchas aplicaciones populares de software no están equipadas con las herramientas necesarias para lograr la conformidad, lo cual lleva a algunas organizaciones a descuidar o ignorar sus propias políticas".

Los mercados de todos los países se encuentran en la difícil situación de poder responder a esta ley. Dado el imperio económico que representa Estados Unidos, las decisiones tomadas allá tienen una repercusión mundial. No obstante, y como ya fue descrito, las empresas norteamericanas también padecen esta problemática de gestión. En Argentina, según un análisis de la consultora Deloitte, el costo para adecuarse a la ley Sarbanes Oxley es superior a los 100 millones de pesos.

La preocupación es clara: la ley Sarbanes Oxley no genera ningún tipo de ingreso económico, y respetarla se convierte en un significativo gasto adicional. En pocas palabras, es una razón para enfurecerse con el Gobierno norteamericano, que tras haber sufrido las estafas millonarias de empresas como Enron, decidió facilitar sus tareas de control delegando gran parte del trabajo a las compañías que quieren operan bajo sus ojos.



"el mundo de **los negocios** cada vez tiene que estar más cerca del **Mundo IT...**" Hugo **Espinoza** Regional Manager para Cono Sur de Citrix

Information Tecnology Infraestructure Library (ITIL): buena literatura

Se lo conoce como el marco de procesos de gestión de servicios en tecnología más aceptado, comprendiendo una lista de mejores prácticas basadas en instituciones públicas y privadas de todo el mundo.

El ITIL consiste en una serie de libros que en su interior desarrollan guías de mejores prácticas orientadas en el accionar de departamentos tecnológicos. Cada libro, que cuesta poco más de U$S 100 y posee más de 200 páginas, explica un ámbito en particular en el cual aplicar metodologías de trabajo. Se identifican 12 procesos, para abarcar el mayor panorama posible de una empresa, cada uno vinculado a la gestión: incidentes, cambios administrativos, finanzas, configuración, realización, nivel de servicios, problemas, continuidad del negocio, disponibilidad, capacidad, seguridad y soporte. Este último es marco de más fácil implementación, y supone la categoría en la que más rápido se aprecian resultados.

Los libros proporcionan útiles modelos de trabajo. Sin embargo, la aceptación de este recurso se está observando en Estados Unidos recién en estos últimos dos años, mientras que su paso por Europa supuso la estadía eterna de numerosos casos de éxito, como ocurrió en su país de origen, Inglaterra, y como está sucediendo en Norteamérica.

La problemática que se observa es que la aplicación de las prácticas de ITIL suponen resultados a largo plazo, es decir, la adopción de una estrategia ITIL, si bien tiene el objetivo de optimizar el tiempo y los recursos, puede tornarse en una seria barrera administrativa a primera vista a raíz de la

dificultad que implica su uso, ya que está afectando a todos aquellos que forman parte de la cadena del negocio en el que se está incorporando; supone en muchas situaciones, cambios drásticos de las formas de trabajo. Además, se basan en frameworks, estructuras de gestión que no necesariamente tienen que aplicarse obligatoriamente a todas las empresas. Tiene que estudiarse cada situación en particular, y analizar entonces el modo en que las prácticas ITIL pueden ser de beneficio propio.
Para la consultora Forrester, la aplicación de estas guías y el creciente interés hacia las mismas es inminente, cuando las compañías se encuentran en mercados cada vez más competitivos y controlados por regulaciones como Sarbanes Oxley.



ISACA e ISC2: capacitarse es la clave

ISACA (Asociación de Auditoría y Control de Sistemas de Información): iniciativa que nació en 1967 cuando un grupo de profesionales del sector TI decidieron desarrollar una guía de referencia central a la que todos pudieran consultar. Actualmente, más de 50 mil miembros en todo el mundo confían en las pautas de gobernación, control, seguridad y auditoría de información.
ISACA se constituye de 170 sedes representativas que están situadas en más de 60 países. En Argentina, aparece ADACSI, que desde su sitio en Internet proporciona información sobre sus actividades locales.
La diversidad de usuarios y el alcance global de los estudios sobre los cuales se basa ISACA son los aspectos más destacables de esta firma, que se halla dirigida principalmente a aquellos profesionales y empresas relacionadas con sistemas de auditoría y análisis de la información. ISACA ofrece las certificaciones, en el ámbito de la seguridad, CISA y CISM. La primera apunta a auditores, mientras que la segunda se dirige a administradores.
Por su parte, ISC2 es un organismo internacional fundado en 1996 que lleva adelante certificaciones dentro del campo de los sistemas de seguridad. Pensada para profesionales en seguridad, ISC2 provee nuevas herramientas para realizar acciones de protección en las empresas. ISC2 brinda capacitación en seguridad informática a profesionales del ámbito tecnológico. De este modo, se distinguen las clases CSSCP, que engloba a administradores de sistemas y networking, y CISSP, que comprende a diseñadores de políticas y procesos de seguridad.



Según un estudio de la consultora IDC e ISC2, Europa va a necesitar más de 650 mil nuevos expertos en seguridad de la información para el 2008. El hecho de contar con calificaciones como las descriptas resulta clave para el 93% de los directivos a cargo de la selección del personal.

Hospitales presionados por HIPAA y el uso de la tecnología

Health Insurance Portability and Accountability Act (HIPAA) es una ley norteamericana que se hizo pública en 1996 con el fin de mejorar y garantizar la información y continuidad de los servicios relacionados a planes de salud. Sin lugar a dudas, el sector de la salud es uno de los mayores espacios en los que se observa la presión ejercida por las reglas de control de los Estados Unidos, particularmente a partir de la ley HIPAA. No obstante, el riguroso monitoreo que se exige sobre la asistencia médica ha sido un impulsor del uso de herramientas tecnológicas que, en última instancia, resultan de beneficio para el hospital y sus visitantes.
Una encuesta reciente realizada y presentada por el Healthcare Information and Management Systems Society en su conferencia anual, revela como los hospitales se inclinan de lleno a la adopción de herramientas informáticas para mejorar sus servicios. Los datos, que reflejan las opiniones 200 ejecutivos relacionados con la asistencia médica, muestran que los Sistemas de Registro Electrónicos Médicos (ERM) son la elección básica, quedando fuera apenas el 17% -el 40% ya está trabajando o se encuentra en la etapa de instalación de una aplicación ERM-. Este tipo de programas está diseñado para llevar un amplio archivo de los pacientes. La implementación de redes de alta velocidad comprende un 93% de los CIOs encuestados, mientras que los sistemas de Intranet y las soluciones de información inalámbricas se llevan cada una un 84% de los votos. Paralelamente, dos tercios de los ejecutivos tienen la confianza de que los presupuestos en IT aumentarán en los próximos 12 meses. Asimismo, el interés hacia soluciones de Outsourcing está al día, en especial aplicaciones de dictado y transcripción así como opciones para establecer mesas de ayuda. El análisis completo puede leerse en www.himss.org/2005survey/.

La realidad del reto tecnológico

Para Hugo Espinoza, Regional Manager para Cono Sur de Citrix, el desafío fundamental que afrontan los mercados es el hecho de poder ver "la tecnología internalizada en el proceso de negocios en la organización, y como parte de la cultura de la gente. Es una cuestión que está sostenida en el tiempo, pero que uno no hace preocupándose del día a día o mientras apaga los incendios normales que tiene la operatividad de la compañía, sino el que está demás alineando los proyectos tecnológicos con aquellos de negocios de la organización, y en ese sentido, es clave ver donde se aplica valor y tecnología en el negocio".
Omar Arab, CEO de Modena Technologies Capital Partners, piensa que "el mundo de los negocios cada vez tiene que estar más cerca del mundo de IT, y que ambos deben interactuar en tiempo real. Para ésto, los sistemas tienen que ser cada vez más adaptables al mundo de los negocios, y por tal motivo trajimos una compañía de agentes inteligentes, Agentis Software, que según la consultora Gartner es la tecnología número uno del mundo. Creo que el mundo de IT se encamina hacia el desarrollo de aplicaciones orientadas a servicios, uno de los pilares de la tecnología de agentes".
La implementación de soluciones tecnologicas es un camino real de crecimiento, tanto para la pequeña como para la gran empresa. Pero es más valioso el conocimiento que tienen aquellos que trabajan con las herramientas digitales, y por ello es que son los usuarios quienes le dan valor a la aplicación informática, más allá del costo y las características que ofrezca -si no se sabe usarla de manera óptima, la tecnología será un nuevo problema con el que la compañía tendrá que lidiar-.
Marcelo Lozano explica que "el análisis del caos en los negocios y la tecnología, lleva a dividir al mundo entre newtonianos y darwinianos. Los primeros fueron los fundadores de la revolución industrial, los que mantuvieron el concepto de infraestructura como valor de una acción, mientras que los segundos son los empresarios que hoy mejor se desempeñan. En Argentina -a la hora de hablar de tecnología- la mayor parte de los empresarios son newtonianos y les cuenta invertir en el cambio, apostar a la innovación como forma de dar valor a su empresa. No logran comprender que el verdadero valor de su empresa es la suma del IQ de quienes la componen, y no pagan el talento. Siguen sin entender que el valor es el conocimiento, la creatividad y el talento para adaptarse a un mundo agresivo, corrosivo y letal".
Las regulaciones, certificaciones y guías de negocios IT que hemos analizado son sólo algunas de las propuestas que hoy existen, y a las que debe acompañarse un continuo desarrollo cultural en base a las herramientas de la empresa. Cada compañía tiene que evaluar sus necesidades, los aspectos que desea mejorar y el mercado en el que está inmersa, para de este modo ser capaz de proveer los beneficios de la adopción de nuevas soluciones tecnológicas. En NEX IT Specialist continuaremos abordando estos temas, que actualmente son claves para pequeñas, medianas y grandes empresas.



BREVES

Acerca de "The Cable Guy"



Conecte su red usando tecnologías Microsoft

En Internet uno puede encontrar buenos productos pero los hay malos y muy malos. Con los artículos técnicos y los escritores de artículos técnicos ocurre lo mismo. En el caso particular del mundo Microsoft aparecen en muchas ocasiones artículos firmados o presentados por "The cable Guy" (el tipo de los cables).
Sus artículos son excelentes. Pero ¿Quién está detrás de "The cable guy"?.
Los artículos de "The cable guy" están escritos por Joseph Davies, un escritor técnico del Grupo Windows Networking and Devices de Microsoft. Su experiencia en TCP, Networking es extensa habiendo escrito artículos, libros y material para curso de todos los niveles. Su último artículo trata de IPSEC y apareció en el sigue de Febrero 2005 del security newsletter.

http://www.microsoft.com/technet/technetmag/issues/2005/05/SecurityWatch/default.aspx

Paradoja del Cumpleaños

De Wikipedia

La paradoja del cumpleaños establece que si hay 23 personas reunidas hay una probabilidad del 50,7% de que al menos dos personas de ellas cumplan años el mismo día. Para 60 o más personas la probabilidad es mayor del 99%. Obviamente es casi del 100% para 366 personas (teniendo en cuenta los años bisiestos). En sentido estricto esto no es una paradoja ya que no es una contradicción lógica; es una paradoja en el sentido que es una verdad matemática que contradice la común intuición. Mucha gente piensa que la probabilidad es mucho más baja, y que hacen falta muchas más personas para que se alcance la probabilidad del 50%.

Ataque del Cumpleaños

El ataque del cumpleaños es un tipo de ataque criptografico que explota las matemáticas detras de la paradoja del cumpleaños haciendo uso de la relación entre tiempo-espacio.

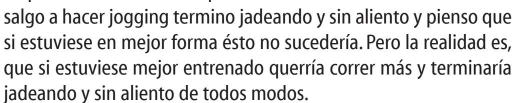
(Más en próximo NEX IT Specialist #24)

Sabía qué...?

De dueño de Thawte, a astronauta, a fundador de Ubuntu....

Mark Shuttleworth fue el fundador de Thawte (la primera "Autoridad Certificante" que vendió certificados públicos SSL).
Después de vender Thawte a Verisign, se fue a Rusia a entrenar como astronauta y visitó el espacio. Cuando retornó fundó Ubuntu (la distribución GNU/Linux más vigente).

Ante la pregunta sobre qué lo conduce hacia estos desafíos responde: "Cada vez que salgo a hacer jogging termino jadeando y sin aliento y pienso que si estuviese en mejor forma ésto no sucedería. Pero la realidad es, que si estuviese mejor entrenado querría correr más y terminaría jadeando y sin aliento de todos modos.



Mark realizó en Python una implementación de RSA de firma digital que OpenSSSL verificaría. Es de origen Sudafricano y hoy vive en Inglaterra.





Buena Impresión



En "Graphics of the Americas", en Miami, HP presentó sus línea de soluciones para impresión digital de gran formato. Las HP Designjet series 8000s y 9000s brindan nuevas oportunidades de negocio a los proveedores de servicios de impresión y los establecimientos de rotulación actuales mediante el uso de tecnología de tinta a base solvente, que permiten un ahorro considerable en sustratos de impresión para formatos para uso de alta durabilidad.
También presentó su nueva impresora de altas prestaciones HP Designjet 4500, diseñada para altos volúmenes de producción a color de formato ancho que ofrecen a los impresores comerciales, diseñadores gráficos, agencias de publicidad, artistas y fotógrafos profesionales nuevas oportunidades de negocio.
HP también estuvo presente con la línea de prensas digitales HP Indigo,
tanto para impresión comercial como la HP Indigo 5000 como la HP Indigo 4050
orientada el mercado de etiquetas.
Estas soluciónes de alta productividad les permite a estas empresas incrementar su volumen de negocio en base a su capacidad expandida de entrada y salida, impresión económica a color, operación independiente y configuraciones opcionales de escaneo / copiado y multifunción.

Humor - *Por Severi*

